(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 February 2013 (07.02.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/017176 A1

(51) International Patent Classification:
H04W 76/02 (2009.01)

(21) International Application Number:
PCT/EP2011/063477

(22) International Filing Date:
4 August 2011 (04.08.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SACHS, Joachim** [DE/DE]; Viktoriaallee 23, 52066 Aachen (DE). **REMBARZ, Rene** [DE/DE]; Anne-Frank-Str. 14, 52064 Aachen (DE). **CATREIN, Daniel** [DE/DE]; Kiefernstr. 9, 52146 Würselen (DE).

(74) Agents: **MEDAU, Joern** et al.; Ericsson Allee 1, 52134 Herzogenrath (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: PROVIDING CONTENT RELATED QUALITY OF SERVICE IN PACKET SWITCHED COMMUNICATION NETWORK

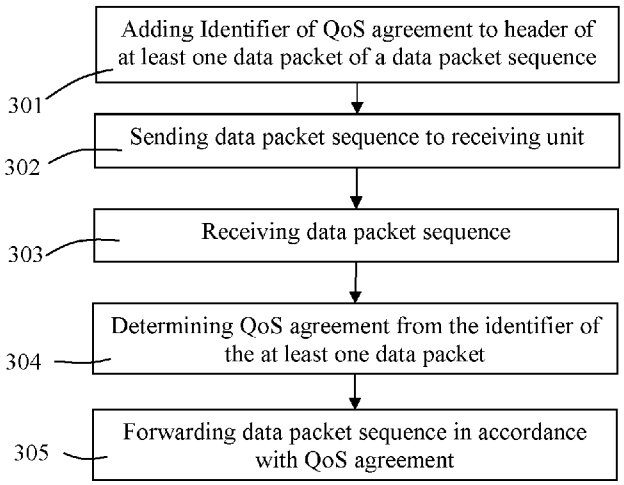

Fig. 3

(57) **Abstract**: A method of establishing a data bearer (207) between a network node (212, 504, 600) of a PS communication network (202) and a mobile station (201, 501, 800) which is attached to the PS communication network (202), wherein the data bearer (207) is established in accordance with a Quality of Service, QoS, agreement associated to the provision of a content to the mobile station (201, 01, 800), the method comprises the following steps: -adding an identifier, identifying the QoS agreement, to at least one data packet of a data packet sequence associated with the content; -sending the data packet sequence to the network node (212, 504, 600); -detecting, by the network node (212, 504, 600), the identifier of the at least one data packet of the data packet sequence; -establishing the data bearer (207) in accordance with the QoS agreement.

WO 2013/017176 A1

Providing content related quality of service in packet switched communication network

Technical Field

This invention is related to the handling of quality of service (QoS). The invention is further related to a method and nodes for providing content to a mobile station, which is attached to a packet switched, PS, mobile communication network, by sending a data packet from a server of the content provider to the mobile station.

Background

Over the years, a rapid growth of mobile broadband subscribers has been recognized by the network operators. At the same time, the traffic volume per subscriber is also increasing rapidly, in particular, with the introduction of flat-rate tariffs and more advanced mobile services. Operators are moving from a single-service offering in the packet-switched domain (e.g. Internet access) to a multi-service offering by adding new services, such as multimedia telephony and mobile-TV, across the mobile broadband access. These services have different performance requirements, for example, in terms of required bit rates and packet delays. Hence, there is a need to standardize simple and effective Quality of Service (QoS) mechanisms for multi-vendor mobile broadband deployments. Such QoS mechanisms should allow the operator of a communication network to enable service differentiation and to control the performance experienced by the packet traffic of a certain service and subscriber group.

The QoS and policy handling in the Third Generation Partnership Project (3GPP) has evolved with different features and different architectures. Detailed information about QoS handling in evolved packet switched networks can be derived from the 3GPP standards TS 23.401, TS 23.402 and TS 36.300. The basic paradigm of QoS support in 3GPP networks is according to

relationships between the end user and the access network provider. This relationship can be static, e.g. according to a contract between the end user and the access network. The QoS profile for the user is then typically stored in a subscriber profile database. Further the relationship can be negotiated dynamically, e.g. when a data session is started which may lead to a special charging for a specific QoS treatment. The dynamic negotiation can also be combined with a long-term policy profile.

According to a negotiated or static QoS profile a QoS bearer can be established within the access network and via the radio interface to the user device. A QoS bearer determines the packet forwarding treatment in the different nodes of the access network and the user device which enables to ensure a common service performance. A QoS bearer can affect e.g. the priority of packet treatment, the reserved resources and also adaptive bearer configuration like channel coding, scheduling priority or power control. There may be multiple QoS bearer that can be setup by the access network for a specific user. Several bearer QoS parameters are known in the state of art. One parameter is the allocation retention priority (ARP) which specifies the relative importance compared to other Radio access bearers for allocation and retention of the Radio access bearer. Other parameters of a bearer QoS is the maximum bit rate (MBR) or the guaranteed bit rate (GBR). Packet filters which might be allocated in the user device for uplink traffic and in the access network for downlink traffic determines which data packet is sent via which data bearer. These traffic filters can be statically configured or they can be dynamically agreed whenever a new data session is set up.

In the already known 3GPP network architecture, 3GPP network operators have pursued the so-called “walled garden approach” in which the users of their networks only having access to the operator-provided and operator-controlled services. One reason for this approach is to keep the operator in the value chain and ensure proper service experience and customization.

Fig. 1 depicts a block diagram of a quality of service treatment of data traffic between a content provider 103 and user equipment 101 according to the

state of art. The mobile subscriber or user equipment 101 is attached to a packet switched (PS) mobile communication network via a radio network. The PS mobile communication network and the radio network are depicted as an access network 102 without mentioning any further details. The user equipment 101 is connected to an access network 102 using different bearers 107, 108 and 109. A quality of service is defined between the subscriber of the user equipment 101 and the access network 102 as a user profile and is stored in a subscriber profile database 104 which is located inside the access network 102. The definition of a QoS can be static according to a long term contract between the subscriber of the user equipment 101 and the operator of the access network 102. The definition of the QoS can also be negotiated 105 dynamically between the subscriber of the user equipment 101 and the operator of the access network 102 when e.g. a data session is started. It is also possible that a combination between a long term contract and a dynamic negotiated QoS definition exists. According to the negotiated QoS treatment a QoS bearer 107 is established 106 within the access network 102 to the user equipment 101. The QoS bearer 107 determines the packet forwarding treatment in the different nodes of the access network 102 and the user equipment 101 which enables to ensure certain service performance via preferred treatment, priority handling of data packets, reserving resources and possibly also adaptive bearer configuration like channel coding, scheduling priorities, power control, etc.. There may be multiple QoS bearers 107, 108, 109 that can be setup by the access network 102 for a specific subscriber or user equipment 101. Packet filters in the access network 102 for downlink traffic and in the user equipment 101 for uplink traffic determine which data packets are sent via which transport bearer 107, 108, 109. These packet filters can be statically configured or dynamically agreed whenever a new data session is setup. After the QoS bearer is setup, data traffic 110 is routed via the access network 102 between the subscriber of the user equipment 101 and the content provider 103.

With the uptake of Internet services, most operators have gradually relaxed this policy and also allow access to so-called “over-the-top” (OTT) services on the Internet. To ensure a proper transmission of packet data from an OTT

service to a user of a communication network there is a need to give the OTT service provider access to the QoS control in the communication network of the network operator so that the OTT service provider can influence the QoS of a provided service. The implementation of this feature is very difficult because the 3GPP networks have been designed with an operator-controlled QoS model without supporting other approaches.

Typical content distribution architectures are distributed over a huge amount of servers with different addresses (like IP addresses) which make it very difficult to store each address of each service providing server in a communication network, especially in light of cloud-based distribution concepts where servers and network addresses are frequently changed. It is therefore not feasible to use addresses of OTT services to map the service with a specific QoS bearer in a mobile communication network because a large database must be used to store every address of servers in combination with changing OTT services.

To circumvent the unreliable address inspection of data packets, it is possible to perform a packet inspection for each data packet to derive information about the OTT service. The data packets consist of several secondary header information and payload data which provide information about the OTT service. As an example, an IP data packet comprises additional TCP or UDP header and could also comprises Hypertext Transfer Protocol (HTTP) data or Extensible Markup Language (XML) information. This method is very time-consuming because the inspection mechanism must be very flexible to cope with different situation. This could lead to a high delay in the transport of inspected data packets.

Thus a flexible mechanism is required that overcomes the mentioned drawbacks from the state of art.

Summary

It is an object of the present invention to improve the content related quality of service in packet switched communication network. This object is achieved by the independent claims. Advantageous embodiments are described in the dependent claims.

The inventions relates to a method of establishing a data bearer between a network node of a PS communication network and a mobile station which is attached to the PS communication network. The data bearer is established in accordance with a Quality of Service, QoS, agreement associated to the provision of a content to the mobile station. The method comprises the step of adding an identifier, identifying the QoS agreement, to at least one data packet of a data packet sequence associated with the content. A further step comprises sending the data packet sequence to the network node. In a further step the network node detects the identifier of the at least one data packet of the data packet sequence and establishes the data bearer in accordance with the QoS agreement.

The invention relates further to a method of providing a content of a content provider to a mobile station. The mobile station is attached to a packet switched, PS, communication network. A data bearer is established between a network node of the PS communication network and the mobile station in accordance with a Quality of Service, QoS, agreement associated to the provision of the content. The method comprises the steps of adding an identifier, identifying the QoS agreement, to at least one data packet of a data packet sequence associated with the content and sending the data packet sequence to the network node. The network node detects the identifier of the at least one data packet of the data packet sequence and determining the corresponding data bearer and maps the data packet sequence to the data bearer associated with the QoS agreement. In a further step the network node transmits the data packet sequence across the PS communication network to the mobile station via said data bearer.

It is possible that this specific one data packet which contains the identifier will not be transmitted over the corresponding bearer which has been established

due to the identifier but over a default bearer. This might happen because the transport delay will be too high if the forwarding of this data packet has to stop until the new bearer has been established.

A packet data sequence in the meaning of this invention consists of at least one data packet and is associated with the content of the content provider. The data packet sequence represents a content or part of content. Further the content is also related to messages which will be sent from the content receiving entity to the content provider (e.g. request messages or acknowledge messages). Another example for a message which will be sent from the content receiving entity to the content provider is a message related to an upload service (e.g. photobook).

In a further embodiment the identifier can be added by a server of the content provider to the at least one data packet of a data packet sequence. It is also possible that the identifier will be added by the mobile station to at least one data packet to establish the data bearer for the following data traffic which is related to this specific communication. This can e.g. be done in one data packet of a request message which might be sent from the mobile station to the content provider to request a service or content. The mobile station may receive the identifier from the content provider e.g. via a downloadable application that is provided by the content provider to the mobile station.

An advantage of the invention is that the content which is sent by the server of the content provider to the mobile station can be transferred through a communication network of a network operator in accordance with an agreement between the content provider and the operator of the network so that the operator of the network is in control of a quality of service for a content which is provided by an external content provider. In one example the mobile subscriber has to pay for a specific quality of service. Another example is that the content provider pays for the provision of content to the operator of the network. The determination of content which is in accordance with the agreement by an identifier is very fast because no deep packet inspection has to be performed. Because not every data packet of a data packet sequence of

the content is marked with the identifier, the mapping of the data packet sequence is very fast and does not need high processing capabilities.

In a further embodiment the invention further comprises the steps of communicating authentication information between the content provider and the network operator, adding a secure tag to at least one data packet of the data packet sequence which is based on the authentication information and verifying, by the network node, that the secure tag is based on the authentication information.

The advantage is that only a certified server of a content provider can use a better QoS for transmitting its content to the mobile subscriber. No unauthorized data packet sequence is accepted by the network node for the specific bearer according to the QoS agreement.

The invention further relates to a network node and a server of the content provider which are adapted to perform the steps of the prescribed methods.

Brief Description of the Figures

Fig. 1 shows a block diagram of a quality of service treatment of data traffic between a content provider and user equipment according to the state of art;

Fig. 2 shows a block diagram of a quality of service treatment of data traffic between a content provider and user equipment according to an embodiment of the invention;

Fig. 3 shows a flow chart according to a first embodiment of the invention;

Fig. 4 shows a flow chart according to a second embodiment of the invention;

Fig. 5 shows an exemplary sequence diagrams according to one embodiment of the invention;

Fig. 6 shows a network node according to one embodiment of the invention;

Fig.7 shows a server of a content provider according to one embodiment of the invention.

Detailed Description

Fig. 2 shows a block diagram of a quality of service treatment of data traffic 210 between a content provider 203 and user equipment 201 according to an embodiment of the invention. The content provider can e.g. be a provider of a newspaper or any other kind of service provider. The content provider 203 can be split up in several servers 213 which are adapted to provide contents or part of the content to other users 201. A user which can be any kind of mobile subscriber using a mobile device which is adapted to provide the requested content to the user (e.g. a smart phone or a mobile computer). The mobile subscriber 201 is attached to a packet switched (PS) communication network 202. The PS communication network 202 can be a mobile communication network or a wireline communication network. As a mobile communication network it also contains the radio network. The PS communication network is depicted as an access network 202 without mentioning any further details.

A business-to-business agreement was concluded between the operator of the access network 202 and the content provider 203 and is stored as a B2B profile in a database 204 in the access network 202. This agreement fixed a quality of service for specific contents of the content provider 203. The database 204 can also be located outside the access network 202 but it has to be queried from the nodes in the access network 202.

The user equipment 201 is connected to the access network 202 using different bearers 207, 208 and 209. According to the B2B agreement a QoS

bearer 207 is established 206 within the access network 202 between a gateway node 212 of the access network 202 and the user equipment or mobile subscriber 201. The QoS bearer 207 determines the packet forwarding treatment in the different nodes of the access network 202 and the user equipment 201 which enables to ensure certain service performance via preferred treatment, priority handling of data packets, reserving resources and possibly also adaptive bearer configuration like channel coding, scheduling priorities, power control, etc.. There may be multiple QoS bearers 207, 208, 209 that can be setup by the access network 202 for a specific subscriber or user equipment 201. One of the bearers 208, 209 can be used for a default setup so that even if there is data which is not related to a QoS agreement can be transferred through the access network 202. This default bearer normally provides a smaller bandwidth than the bearers which have been associated to a QoS agreement. It is also possible that the default bearer provides the remaining bandwidth which is not used by other bearers.

In Fig. 2 the data traffic 210 is routed through the access network over a QoS bearer 207 which is in accordance with the B2B-QoS agreement stored in the database 204. Between the node 212 of the access network 202 which can be e.g. a gateway node (GGSN) of a GPRS network or any other kind of gateway node of a packet switched access network and the server 213 of the content provider 203 the data traffic can be routed through different networks like the Internet or other mobile networks.

Fig. 3 shows a flow chart according to one embodiment of the invention. In a first step 301 a server of a content provider adds an identifier to the header of at least one data packet of a data packet sequence which has to be sent to a mobile subscriber according to a quality of service agreement. The data packet sequence comprises at least one data packet and is defined as an equal set of data packets wherein some of the header fields are the same (e.g. network addresses of the destination and origination). To reduce overhead data and required processing capacity it is possible not to add the identifier to every data packet of the data packet sequence but to just add the identifier to the first data packet of the data packet sequence or to add the

identifier to every predefined number of data packets in the data packet sequence. The QoS was agreed between the content provider and the operator of the access network of the subscriber. This identifier identifies the QoS agreement such that if there are existing more than one agreement between the content provider and the operator of the access network, a specific agreement is identified. This can e.g. be done by a specific number which is allocated to this specific agreement.

In a next step 302 the data packet sequence is sent to a receiving unit of the access network in which the subscriber has its subscription. A receiving unit can be any kind of gateway node of the access network. After the receiving unit receives the data packet sequence in a further step 303 the QoS agreement is determined in a next step 304 based on the identifier of at least one data packet of the data packet sequence which was added by the server of the content provider in step 301. In a further step 305 the data packet sequence is mapped to a bearer in accordance with the QoS agreement and is then forwarded towards the subscriber over said bearer.

If the bearer does not exist the network node will establish the data bearer between the network node and the subscriber first. Because it might take time to establish the bearer the data packet sequence or the data packet which contains the identifier will be forwarded over a default bearer first. After the data bearer is established in accordance with the QoS agreement the remaining data packets of the data packet sequence and all the following data packet sequence which are associated to the content can be sent over this new established bearer.

In one embodiment the network node remains the established bearer 207 which is in accordance with QoS agreement for a predefined time so that if the network node, after transmitting a first data packet sequence or stream over the established bearer 207, receives a second data packet sequence which is also allocated to the QoS agreement it is able to transmit the second data packet sequence to the already established data bearer 207 without checking the identifier in the at least one data packet.

In a further embodiment of the invention according to Fig. 4 the server of the content provider, after the identifier according to the QoS agreement has been added to at least one data packet of a data packet sequence or stream in a first step 401, creates a secure tag based on a HASH algorithm in a step 402. The HASH algorithm is performed over a specific part of the at least one data packet (header, payload or a combination of both) and can be based on authentication information which has been communicated between the content provider and the operator of the access network before. The key may be based on symmetric encryption with shared keys or on asymmetric encryption with public and private key pairs. In the symmetric encryption the keys have to be exchanged on a secured communication between the operator of the access network and the content provider. The asymmetric encryption is based on an unsecured transmission of a public key which is allocated to a private key so that both keys are part of a key pair. The private key will not be transferred to other participants. The sender which can be the mobile subscriber or the server of the content provider will add a fingerprint or tag to the message by using its private key wherein the receiver of this message can check the validity of the identity of the sender with the public key received from the sender before. However it is possible for a skilled person to apply the principle of symmetric or asymmetric encryption on this embodiment of the invention. Further integration of processes of automatic distribution of keys to new content providers, key renewal procedures have not been described in this invention and can be implemented accordingly.

The implementation of the secure tag into a header of at least one data packet of a data packet sequence can be performed by using an IPv6 extension header to convey the tag. Another possibility to include the secure tag into the header is to define a new header or to use an existing and already defined header, e.g. the destination options header, to convey the tag. It needs to be ensured that the content provider shall be able to create valid data packet or IP packet tags and that it shall not be possible to re-use already created tags by the content provider for other data packets than the ones originally tagged. To fulfill such security requirements the creation of the secure tags can be based on a HASH-based message authentication code (HMAC) such as

HMAC-SHA-1 and HMAC-MD5. These algorithms are well established fast and secure HASH-algorithm. It is also possible to use another security algorithm. Furthermore the tag may contain an indicator which indicates the parts of the data packet which have been used for calculation of the tag. It is also possible that the tag may include an indication of the key which has been used to calculate the tag. This is necessary when more than one key is used at the same time for the same service. To ease the processing on the access network side it is possible to mark the header of the at least one data packet of the data packet sequence to indicate that this data packet contains a secure tag. This can e.g. be done in the traffic class field or in the flow label fields of the IPv6 header. It is possible that not each data packet of a data packet sequence contains this secure tag.

After the secure tag is added to the header of the at least one data packet in step 403 the data packet sequence is sent to the receiving unit in step 404.

In step 405 a gateway node of the access network of the mobile network operator receives the data packet sequence. The gateway node can be e.g. a Packet Data Network Gateway (P-GW) or a Gateway GPRS Support Node (GGSN) of a 3GPP access network or any other kind of gateway node of a packet switched access network.

In step 406 the node determines the QoS agreement based on the identifier of the at least one data packet of the data packet sequence. This determination is also needed to identify the necessary key for the validity check of data packets which were tagged by the secure tag.

In step 407 the node will check the incoming data packet sequence to identify the at least one data packet which has been tagged by the secure tag. If at least one data packet of the data packet sequence is tagged the validity of the tag will be calculated based on the key (symmetric or asymmetric key). Therefore the HMAC over the specific parts of the message (header, payload or a combination of both) will be calculated in step 408. The result will be compared with the HMAC in the tag in step 409. If the both values are the

same the data packet sequence is forwarded in accordance with the QoS agreement using the specific bearer 207 in step 410.

If the result of the comparison step 409 is negative, the data packet sequence can be mapped on a default bearer 208, 209 which is used to transfer all data packets with a lower priority or the data packet sequence will be discarded. Both options are described in step 411 of Fig. 4.

The gateway node might also check the validity of the keys which have been used to create the tag before the data packet sequence is forwarded to the subscriber. This is typically done with a billing or charging system. Depending on the QoS agreement the content provider may have a pre-paid account. The billing/charging system will then immediately deduct the costs for transporting the data packet sequence to the subscriber and approve the validity of the key. For a post-paid account the billing/charging system will aggregate the costs for the transportation of the data packet sequence and the key will automatically be validated. In this case only if the data packet sequence contains at least one data packet with an authorized tag that was created with a valid key the data packet sequence will be forwarded to the subscriber using the QoS in the access network.

Fig. 5 depicts a sequence diagram which shows an embodiment of the invention. A mobile subscriber (MS) 501 is attached to a serving GPRS support node (SGSN) 502 of an access network. A gateway GPRS support node (GGSN) 504 is also located in the access network to establish a connection of the access network to a content providing server (CP-Server) 505 of a content provider. A business-to-business (B2B) profile database 503 can be reached by the GGSN 504. The B2B profile database 504 contains the parameters of a QoS agreement between the content provider and the operator of the access network. The parameters can be e.g. the allocation retention priority (ARP), the maximum bit rate (MBR) or the guaranteed bit rate (GBR). It is possible that not all of the parameters will be used to define a QoS agreement.

After the CP-Server 505 adds an identifier to at least one data packet of a data packet sequence in a first step 506 the data packet sequence is transferred to the GGSN 504. The identifier is determined in a next step 508. Based on the identifier the GGSN 504 interrogates in a next step 509 the B2B profile database 503 to get the relevant parameters of the QoS agreement. Based on this information the GGSN maps the data packet sequence in a next step 510 to a bearer which treats the data packet sequence according to the at least one QoS parameter. The GGSN 504 transmits or bears the data packet sequence in a next step 511 to the SGSN node 502 on the QoS bearer which forwards 512 the data packet sequence to the MS 501. The use of the security tag as described in Fig. 4 can also be implemented in the GGSN 504. This is not depicted in Fig. 5.

It is possible that after the GGSN 504 interrogates the B2B profile database 503 the received parameters might be stored in the GGSN 504 or in a further database to reduce data traffic caused by interrogating the B2B profile database 503. This advantage is caused by the fact that content data which is provided by the CP-server is normally split up in several data packets which all uses the same QoS agreement. The duration of the storage of profile data in the GGSN 504 or in a further database can be limited so that the storage can not be overfilled with profile data.

The server 505 of the content provider can be a specific server which is adapted to handle all outgoing data packets in accordance with the invention. It is also possible that each content providing server 505 of a content provider contains means which are adapted to perform all steps of the embodiments of the invention.

Fig. 6 depicts a network node 600 according to one embodiment of the invention. The network node 600 comprises a receiving unit 601, adapted to receive a data packet sequence and a sending unit 605, adapted to bear the data packet sequence across the PS communication network 202 to a mobile station 201 via a data bearer 207.

Further the network node 600 contains a first processing unit 602, adapted to detect an identifier in at least one data packet of the data packet sequence which is associated to a Quality of Service, QoS, agreement and a second processing unit 604, adapted to map the data packet sequence to a data bearer 207 in accordance with the QoS agreement. Both processing units 602, 604 can be combined in one processor which is divided into several modules or which contains several units which perform the steps.

In a further embodiment the network node 600 comprises an interrogating unit 603, adapted to interrogate at least one quality of service parameter from a database 204 based on the determined identifier. The interrogating unit 603 sends a request message to the database 204 containing an identification of the QoS which have been determined before. The database 204 answers the request and sends back the parameters or the content of the QoS agreement. These contents might comprise a minimum bandwidth or an identifier of a bearer setup used in the PS mobile communication network such that the network node can map the data packet to a bearer 207 which is in accordance with the QoS agreement.

Fig. 7 shows a server 700 according to one embodiment of the invention. The server 700 belongs to a content provider which provides content, like music data, news data or any other kind of data, to a user. The content can be spread over a large number of servers 700 or it can be stored on only one server 700. The server 700 comprises a processing unit 701, adapted to add an identifier to a data packet of a content identifying a quality of service, QoS, agreement associated to the provision of the content. It is possible that a content provider is able to provide different contents to users and each content is associated to a QoS agreement between the content provider and the operator of an access network for the user.

The server can be a specific server which receives e.g. data packets from the content servers. This specific server will then perform the prescribed processes on every data packet which has to be processed in accordance with the QoS agreement. Further the server 700 comprises a sending unit

702, adapted to send the data packet to a network node 212, 504, 600 of the access network 202 for the mobile station 201, 501, 800.

Fig. 8 shows a mobile station 800 which is adapted to receive content from a content provider. The mobile station 800 is attached to a PS communication network and comprises a processing unit 801, adapted to add an identifier to at least one data packet of a data packet sequence, identifying the QoS agreement associated to the provision of the content. A data packet sequence can be a request message which is used by the mobile station 800 to request the provision of content from the content provider. The request message can be integrated into an application (APP) of the mobile station 800 so that a user just has to start this APP to receive content. The mobile station further comprises a sending unit 802, adapted to send the data packet sequence to a network node 212, 504, 600 of the PS communication network 202.

Claims

1. A method of establishing a data bearer (207) between a network node (212, 504, 600) of a PS communication network (202) and a mobile station (201, 501, 800) which is attached to the PS communication network (202), wherein the data bearer (207) is established in accordance with a Quality of Service, QoS, agreement associated to the provision of a content to the mobile station (201, 501, 800), the method comprises the following steps:
   - adding an identifier, identifying the QoS agreement, to at least one data packet of a data packet sequence associated with the content;
   - sending the data packet sequence to the network node (212, 504, 600);
   - detecting, by the network node (212, 504, 600), the identifier of the at least one data packet of the data packet sequence;
   - establishing the data bearer (207) in accordance with the QoS agreement.

2. A method according to claim 1, wherein packet filters are established in the network node (212, 504, 600) and in the mobile station (201, 501, 800) that matches the data packet sequence associated with the content to the established data bearer (207).

3. Method according to claim 1 or 2, wherein the QoS agreement comprises QoS parameters and is stored in a database (204) located in the PS communication network (202).

4. Method according to claim 3, wherein the QoS agreement comprises at least one of the QoS parameters:
   - allocation retention priority (ARP),
   - maximum bit rate (MBR),
   - guaranteed bit rate (GBR).

5. A method of providing a content of a content provider (203) to a mobile station (201, 501, 800) which is attached to a packet switched, PS,

communication network (202), wherein a data bearer (207) is established between a network node (212, 504, 600) of the PS communication network (202) and the mobile station (201, 501, 800) in accordance with a Quality of Service, QoS, agreement associated to the provision of the content, the method comprises the following steps:

- adding an identifier, identifying the QoS agreement, to at least one data packet of a data packet sequence associated with the content;
- sending the data packet sequence to the network node (212, 504, 600);
- detecting, by the network node (212, 504, 600), the identifier of the at least one data packet of the data packet sequence and determining the corresponding data bearer (207);
- mapping, by the network node (212, 504, 600), the data packet sequence to the data bearer (207) associated with the QoS agreement;
- transmitting the data packet sequence across the PS communication network (202) to the mobile station (201, 501, 800) via said data bearer (207).

6. A method according to any of the claims 1 to 5, wherein the step of adding an identifier, identifying the QoS agreement, to at least one data packet of a data packet sequence associated with the content is performed at the server (213, 505, 700) of the content provider (203).

7. A method according to any of the claims 1 to 5, wherein the step of adding an identifier, identifying the QoS agreement, to at least one data packet of a data packet sequence associated with the content is performed at the mobile station (201, 501, 800).

8. A method according to any of the claims 1 to 7, wherein the PS communication network (202) is controlled by a network operator and wherein the QoS agreement is concluded between the content provider (203) and the network operator.

9. Method according to claim 8, further comprises the steps of:

- communicating authentication information between the content provider

(203) and the network operator;

- adding a secure tag to at least one data packet of the data packet sequence which is based on the authentication information;
- verifying, by the network node (212, 504, 600), that the secure tag is based on the authentication information.

10. Method according to claim 9, wherein the data packet sequence is mapped by the network node (212, 504, 600) to a default bearer (208, 209) if the secure tag is not based on the authentication information.

11. Method according to claim 9, wherein the data packet sequence is discarded if the secure tag is not based on the authentication information.

12. Method according to any of the claims 9 to 11, wherein the secure tag is a Hash-based message authentication code, HMAC.

13. Method according to claim 12, wherein the secure tag comprises an indication, indicating which part of the at least one data packet of the data packet sequence is used to calculate the HMAC.

14. Method according to any of the claims 1 to 13, wherein the at least one data packet is an Internet Protocol, IP, packet and the identifier is arranged in the IP-header of the at least one data packet.

15. Method according to claim 14, wherein the IP-packet is in accordance with the IPv6 standard.

16. Method according to claim 15, wherein the identifier is contained in an extension header of the IPv6 header of the at least one data packet.

17. A network node (212, 504, 600) of a packet switched, PS, communication network (202), comprising:

- a receiving unit (601), adapted to receive a data packet sequence;
- a first processing unit (602), adapted to detect an identifier in at least

one data packet of the data packet sequence which is associated to a Quality of Service, QoS, agreement;

- a second processing unit (604), adapted to map the data packet sequence to a data bearer (207) in accordance with the QoS agreement;
- a sending unit (605), adapted to transmit the data packet sequence across the PS communication network (202) to a mobile station (201, 501, 800) via said data bearer (207).

18. Network node (212, 504, 600) according to claim 17, adapted to perform all the steps of the method of at least one of the claims 1 to 16.

19. A server (212, 505, 700) for providing a content to a mobile station (201, 501), wherein the mobile station (201, 501, 800) is attached to a packet switched, PS, communication network (202), comprising:
    - a processing unit (701), adapted to add an identifier to at least one data packet of a data packet sequence of the content, identifying a quality of service, QoS, agreement associated to the provision of the content;
    - a sending unit (702), adapted to send the data packet sequence to a network node (212, 504, 600) of the PS communication network (202).

20. A server (212, 505, 700) according to claim 19, adapted to perform all the steps of the methods of at least one of the claims 1 to 16.

21. A mobile station (201, 501, 800) for receiving a content from a content provider, wherein the mobile station (201, 501, 800) is attached to a packet switched, PS, communication network (202), comprising:
    - a processing unit (801), adapted to add an identifier to at least one data packet of a data packet sequence, identifying a quality of service, QoS, agreement associated to the provision of the content;
    - a sending unit (802), adapted to send the data packet sequence to a network node (212, 504, 600) of the PS communication network (202).

22. A mobile station (201, 501, 800) according to claim 21, adapted to perform all the steps of the methods of at least one of the claims 1 to 16.

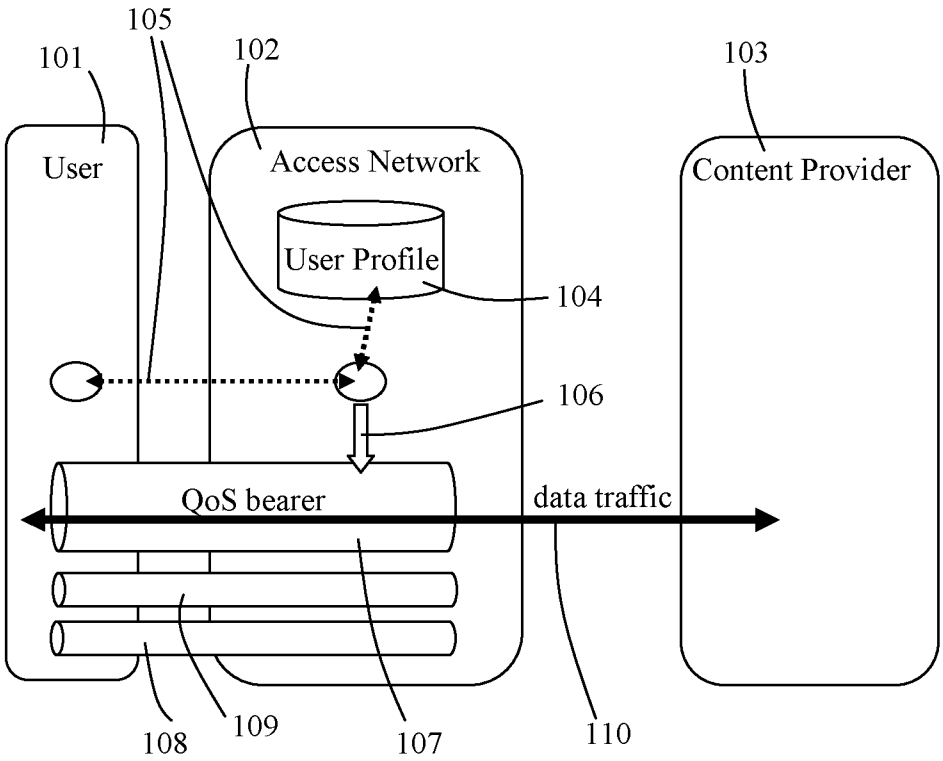
105
101
102
103
User
Access Network
Content Provider
User Profile
104
106
QoS bearer
data traffic
108
109
107
110

Fig. 1

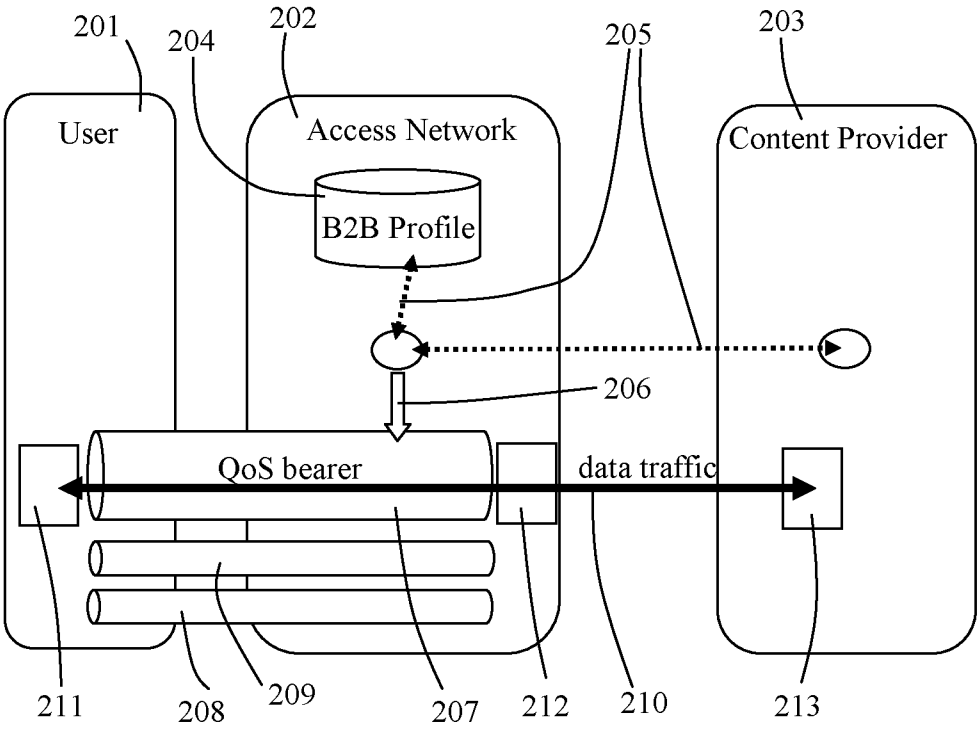
201
204
202
205
203
User
Access Network
Content Provider
B2B Profile
206
QoS bearer
data traffic
211
208
209
207
212
210
213

Fig. 2

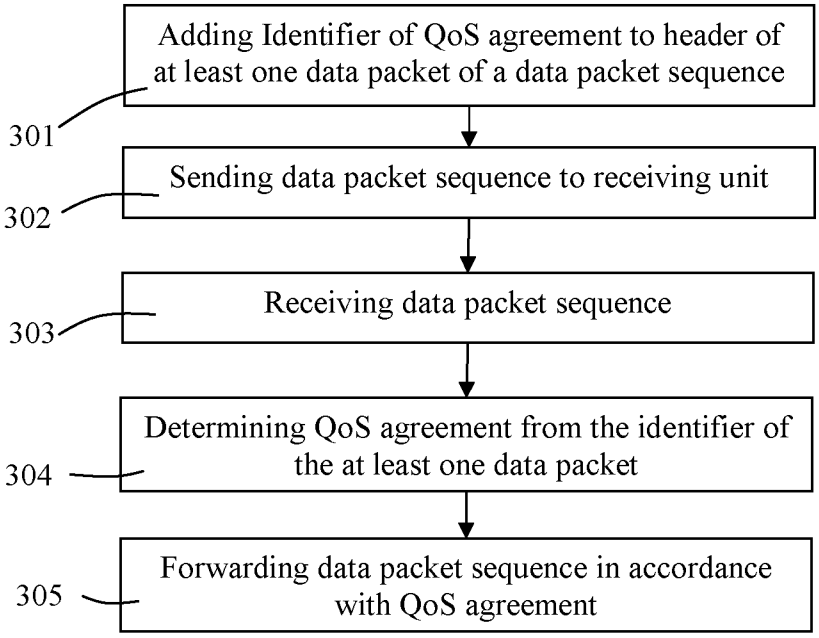
Adding Identifier of QoS agreement to header of at least one data packet of a data packet sequence
301
Sending data packet sequence to receiving unit
302
Receiving data packet sequence
303
Determining QoS agreement from the identifier of the at least one data packet
304
Forwarding data packet sequence in accordance with QoS agreement
305

Fig. 3

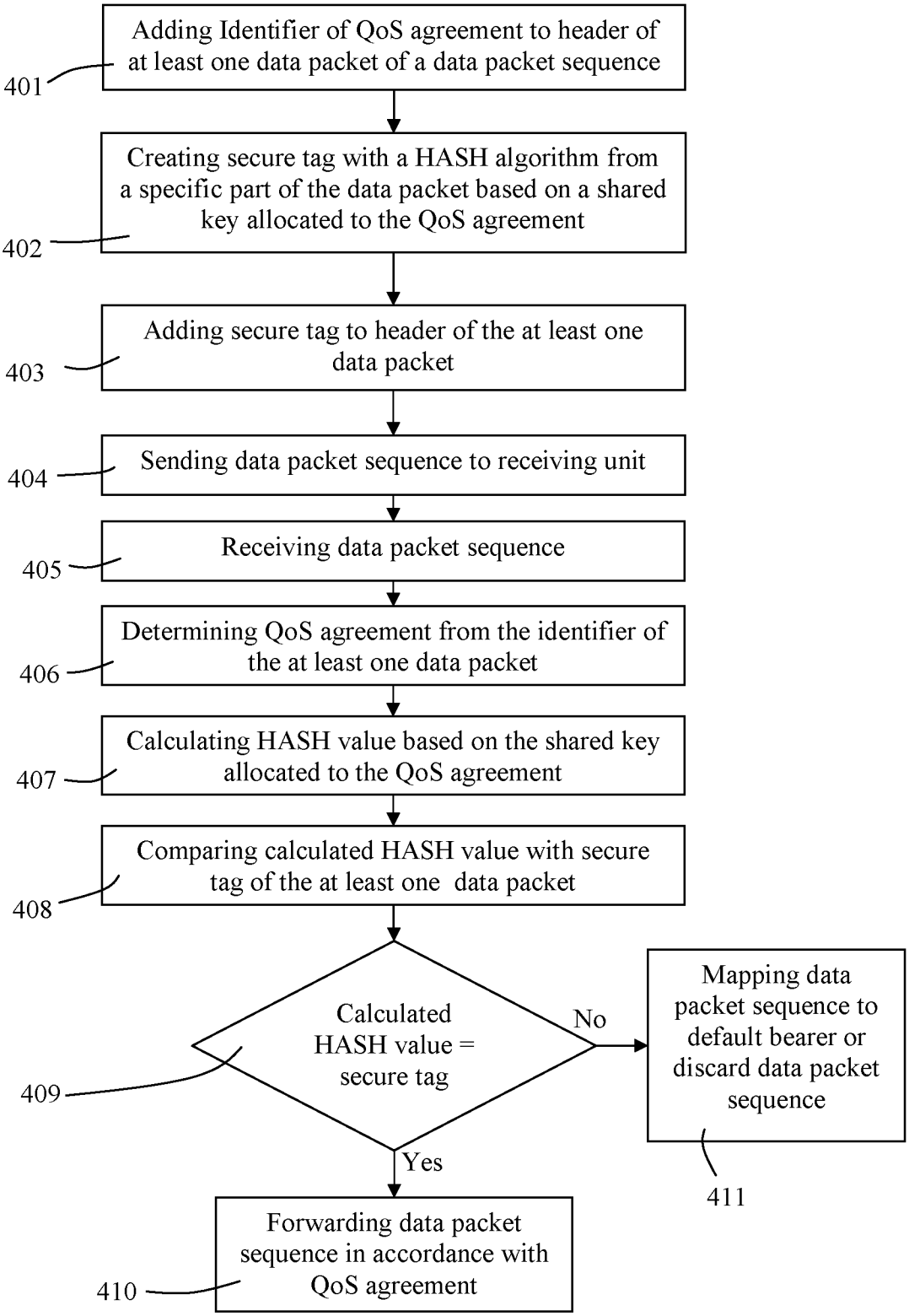
Adding Identifier of QoS agreement to header of at least one data packet of a data packet sequence
401
Creating secure tag with a HASH algorithm from a specific part of the data packet based on a shared key allocated to the QoS agreement
402
Adding secure tag to header of the at least one data packet
403
Sending data packet sequence to receiving unit
404
Receiving data packet sequence
405
Determining QoS agreement from the identifier of the at least one data packet
406
Calculating HASH value based on the shared key allocated to the QoS agreement
407
Comparing calculated HASH value with secure tag of the at least one data packet
408
Calculated HASH value = secure tag
409
No
Mapping data packet sequence to default bearer or discard data packet sequence
411
Yes
Forwarding data packet sequence in accordance with QoS agreement
410

Fig. 4

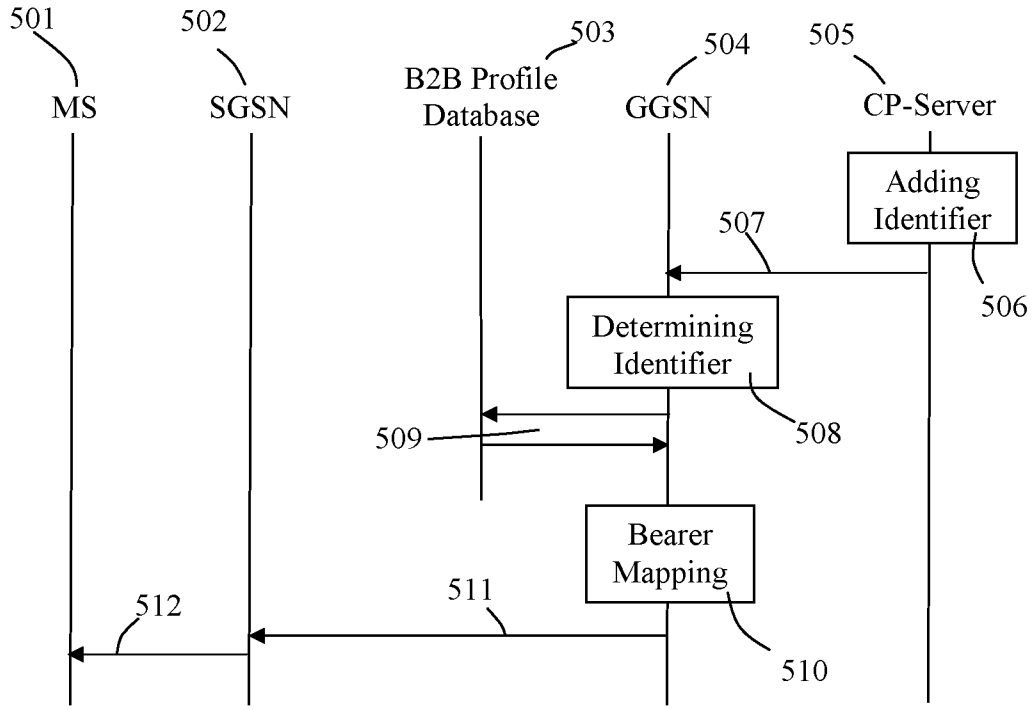
501
MS
502
SGSN
503
B2B Profile Database
504
GGSN
505
CP-Server
Adding Identifier
507
506
Determining Identifier
508
509
Bearer Mapping
511
512
510

Fig. 5

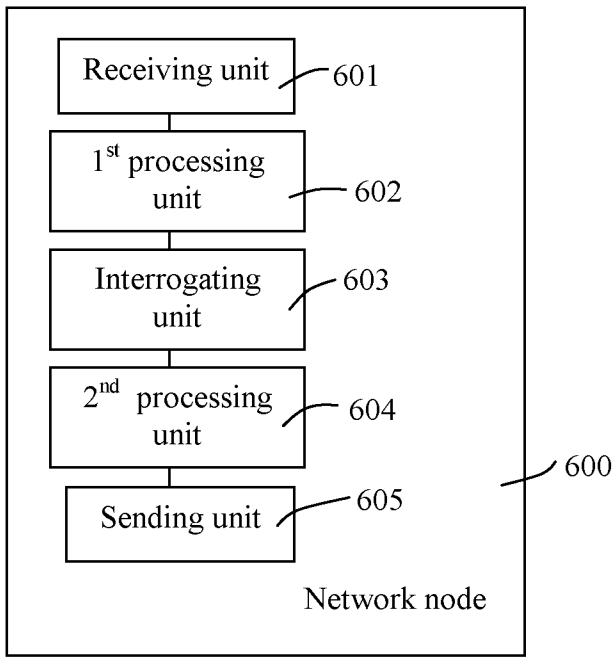

Fig. 6

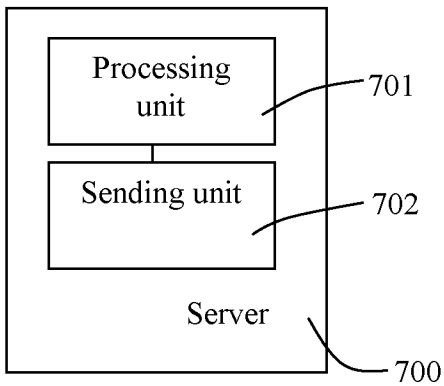

Fig. 7

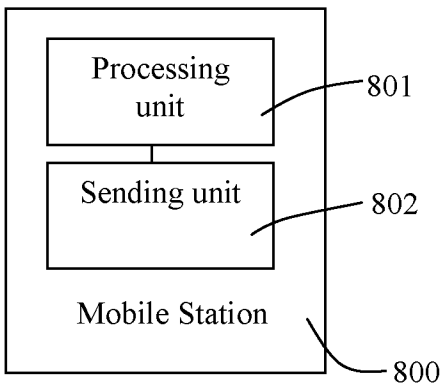

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/063477

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W76/02
ADD.

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)
H04W

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2010/112077 A1 (ERICSSON TELEFON AB L M [SE]; LUDWIG REINER [DE]; EKSTROEM HANNES [SE]) 7 October 2010 (2010-10-07) page 8, line 15 - line 17 page 12, line 6 - page 13, line 25 page 7, line 24 - line 32	1-4, 19-22
X	US 2011/080886 A1 (CHANDRACHOOD SANTOSH [US] ET AL) 7 April 2011 (2011-04-07) abstract paragraphs [0003], [0013], [0021] - [0038], [0040], [0043] - [0045]	1-4, 19-22

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 April 2012	03/05/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Moreno-Solana, S

2

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2010/067400 A1 (DOLGANOW ANDREW [CA] ET AL) 18 March 2010 (2010-03-18) paragraphs [0002], [0013], [0015] - [0021], [0042], [0045] - [0049], [0053], [0054], [0073] figure 1	5,17,18 6-16
Y	US 2011/035495 A1 (EKSTROEM HANNES [SE] ET AL) 10 February 2011 (2011-02-10) abstract paragraphs [0006], [0007], [0014.0020], [0026], [0052] - [0068], [0079]	6-8
Y	US 2009/296702 A1 (STEVENS GILMAN R [US] ET AL) 3 December 2009 (2009-12-03) abstract paragraphs [0010], [0011], [0032], [0033], [0035] - [0041], [0053], [0071] - [0073]	9-16
A	US 2009/252148 A1 (DOLGANOW ANDREW [CA] ET AL) 8 October 2009 (2009-10-08) abstract paragraphs [0006] - [0012], [0030] - [0032], [0039], [0057] - [0064]	5-18
A	BLESS R ET AL: "Secure Signaling in Next Generation Networks with NSIS", COMMUNICATIONS, 2009. ICC '09. IEEE INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 14 June 2009 (2009-06-14), pages 1-6, XP031506415, ISBN: 978-1-4244-3435-0 the whole document	5-18
A	US 2010/212006 A1 (DOLGANOW ANDREW [CA] ET AL) 19 August 2010 (2010-08-19) abstract paragraphs [0027] - [0035], [0046], [0054]	5-18
A	KESHAVA MURTHY K S: "NextGen wireless access gateway analysis of combining WiMAX and LTE gateway functions", INTERNET MULTIMEDIA SERVICES ARCHITECTURE AND APPLICATIONS, 2008. IMSAA 2008. 2ND INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 10 December 2008 (2008-12-10), pages 1-6, XP031408557, ISBN: 978-1-4244-2684-3 the whole document	5-18

-/--

2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/063477

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008/056273 A1 (PELLETIER GHYSLAIN [SE] ET AL) 6 March 2008 (2008-03-06) abstract paragraphs [0017] - [0020], [0069], [0070], [0077]	5-18

2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2011/063477

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-4, 19-22

   Establishing a data bearer between a network node of a PS communication network and a mobile station.

   ---

2. claims: 5-18

   Providing a content of a content provider to a mobile station.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2011/063477

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010112077 A1	07-10-2010	EP 2415216 A1	08-02-2012
		WO 2010112077 A1	07-10-2010
US 2011080886 A1	07-04-2011	NONE	
US 2010067400 A1	18-03-2010	NONE	
US 2011035495 A1	10-02-2011	CN 101401382 A	01-04-2009
		EP 1972120 A1	24-09-2008
		US 2011035495 A1	10-02-2011
		WO 2007079773 A1	19-07-2007
US 2009296702 A1	03-12-2009	US 2009296702 A1	03-12-2009
		US 2011082925 A1	07-04-2011
US 2009252148 A1	08-10-2009	NONE	
US 2010212006 A1	19-08-2010	NONE	
US 2008056273 A1	06-03-2008	EP 2057813 A2	13-05-2009
		US 2008056273 A1	06-03-2008
		WO 2008027005 A2	06-03-2008