Admission Control in IP Multicast over Heterogeneous Access Networks

Pedro Santos
Portugal Telecom Inovação, Aveiro, Portugal
est-p-santos@ptinovacao.pt

Antonio Pinto
Escola Superior de Tecnologia e Gestão de Felgueiras, Politécnico do Porto
INESC Porto, Portugal
apinto@inescporto.pt

Manuel Ricardo
INESC Porto, Faculdade de Engenharia, Universidade do Porto, Portugal
mricardo@inescporto.pt

Teresa Almeida
Portugal Telecom Inovação, Aveiro, Portugal
teresa@ptinovacao.pt

Francisco Fontes
Portugal Telecom Inovação, Aveiro, Portugal
fontes@ptinovacao.pt

Abstract

Network operators have been reluctant to deploy IP multicast services mainly due to the lack of native control over multicast groups. This lack of control does not only prevent operators from generating revenue from multicast-based services but also hinders regular network management. In this work we identified the network elements where admission control should be enforced for multicast session spawning over heterogeneous access networks.

The architecture proposed uses existing AAA functionality to perform user identification and multicast session admission control. This control is made at the network layer with no protocol modifications. Three access networks were considered: xDSL, WiMAX and UMTS.

1. Introduction

IP multicast [6] is an IP packet forwarding technique by which a data stream is delivered simultaneously to a group of users. This is achieved by replicating packets where the path to the group of receivers diverges.

The scalability and bandwidth savings of IP multicast makes it a network technology very attractive to network operators. However, the deployment of IP multicast-based services has been limited in scope. Operators already offer services such as IPTV to their customers, but customers are still unable to be the source of multicast trees, and more dynamic multicast services are not offered. One of the reasons behind this limited adoption is the lack of control network operators have over multicast groups [7]. IP multicast has an open group architecture, where any user is free to receive or transmit data from/to a multicast group. Although this grants high scalability to multicast based services, this openness raises problems for network operators such as access control and traffic accounting. From the operators point of view, AAA multicast capabilities are essential and they must be associated to IP multicast-based services, so that functions such as accounting, billing or regular network management may take place.

Some degree of control over IP multicast groups can be achieved with end-to-end encryption of IP multicast data or IP multicast session access control [16]. While the first solution protects multicast data from unauthorized access and potential eavesdroppers, its use implies high system complexity, such as creation and distribution of encryption keys, and custom software. It does not also prevent a user from joining a group to which he does not have access to, thus causing the unnecessary extension of the multicast distribution tree, which results in wasted bandwidth and wasted computer power. IP multicast session access control, on the other hand, enables network operators to manage IP multicast at a network level by performing access control at the edge-router. Since the edge-router is where IGMP [3] messages are processed, operators are able to identify group ac-

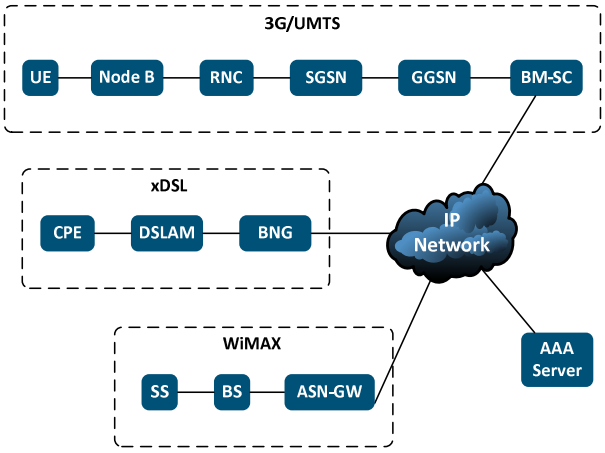

Figure 1. Reference network scenario

cess requests and multicast transmissions; this enables network operators to specify which multicast streams a user can send data to or receive data from.

The remainder of this paper is structured as follows: Chapter 2 presents the reference scenario and current multicast support on relevant access networks; Chapter 3 presents the related work; Chapter 4 presents the proposed solution; Chapter 5 presents the experimental results; Chapter 6 draws the conclusions of this work.

2. Multicast in Access Networks

Multicast support plays an important role in Next Generation Networks (NGNs). Applications such as video broadcasting, streaming, on-line games, may benefit from using IP multicast.

The evolution of access networks towards an all-IP network model demands a unified multicast AAA architecture. Figure 1 illustrates the reference network, and the related network elements this paper focused on. Three access networks were considered: xDSL, WiMAX (802.16d) and UMTS. These networks are interconnected by an IP network and served by a common AAA infrastructure.

2.1. xDSL

The xDSL architecture [5] and respective network elements are shown in Figure 2. The Broadband Network Gateway (BNG) is the IGMP router; its roles are to receive and process IGMP messages and to forward multicast packets. The BNG is also the Network Access Server (NAS) where users authenticate themselves during network attachment.

In xDSL networks, the connections are typically PPPoE being the connection endpoints the Customer Premises

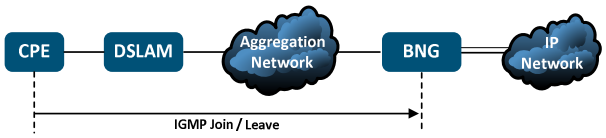

Figure 2. xDSL network architecture

Equipment (CPE) and the BNG. These connections are required for user authentication and authorization during network attachment. The point-to-point nature of these connections implies that the multicast packet replication is performed at the BNG. Although this provides a central point for multicast management, it leads to data redundancy in the aggregation network - multicast packets are replicated on a per PPPoE connection basis, even if the path through the aggregation network is shared by two or more group members. This effectively nullifies the bandwidth savings offered by multicast.

Optimized multicast in xDSL, where all network elements would perform multicast packet replication, requires a migration to Ethernet aggregation and the use of IPoE for multicast data. Additionally, layer 2 equipments such as DSLAMs and switches, should either perform IGMP snooping [4] or function as IGMP proxies [8]. Considering that PPPoE still continues to be used for authentication purposes, optimized xDSL multicast demands the establishment of two network connections: one for typical Internet access (PPPoE), and another for multicast services (IPoE). IGMP messages can be sent through both connections or just through the IPoE connection. When sent through both, the BNG can monitor individual members by correlating IGMP messages with the PPPoE connection from which they were received. When IGMP messages are only sent through the IPoE connection, the BNG may be able to track individual members depending on whether the DSLAM performs IGMP snooping or behaves as an IGMP proxy. IGMP snooping at the DSLAM enables the BNG to identify individual members based on the packets IP or MAC addresses. IGMP proxy, however, prevents BNG from identifying individual group members since the DSLAM, which in this case generates the IGMP messages, would act as an IGMP router for users and as an IGMP client for the BNG.

2.2. WiMAX

WiMAX network architecture [23] is depicted in Figure 2. Before packets can be transmitted, an IEEE 802.16 transport connection must be created between a Base Station (BS) and a Subscriber Station (SS). These connections are identified by a 16-bit Connection ID (CID) number, and by a layer 2 tunnel between the BS and Access Service Network Gateway (ASN-GW). In WiMAX the role of IGMP

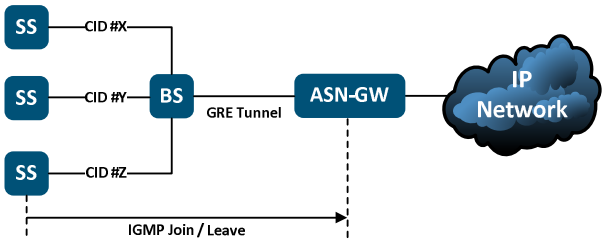

Figure 3. WiMAX network architecture

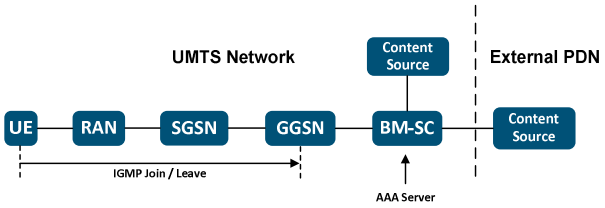

Figure 4. UMTS/MBMS network architecture

router falls upon the ASN-GW network element, which is also responsible for client AAA.

Upstream connections (SS to ASN-GW) are exclusively point-to-point. Downstream connections can be used to transmit data to a group of SSs (under the same BS), using multicast CIDs (mCIDs). Multicast CIDs are therefore suited for IP Multicast data transmission. This solution requires the establishment and management of mCIDs and their associations with IP multicast-based services. These management mechanisms and related protocols are still under development by the WiMAX Forums Networking Group. There are some unresolved issues with the use of mCID [11][15], namely the reduced transmission efficiency of mCIDs for small multicast groups, the missing support for unidirectional broadcast channels, and the existence of additional security threats associated with broadcast channels in a power-conservative wireless system.

2.3. UMTS

UMTS networks, since Release 99, have support for IP multicast. The IGMP router role is performed by the GGSN [2]. IP multicast packet transmission inside the UMTS network is performed over point-to-point tunnels (from the GGSN to the UE), thus no sharing gains are achieved. In Release 6, the Multimedia Broadcast/Multicast Service (MBMS) [1] was introduced with the purpose of supporting native multicast transport connections within the UMTS network (see Figure 2).

MBMS adds a new network element to the UMTS network, the BM-SC (Broadcast/Multicast Service Center), which is the central point for MBMS management decisions. Its functions include MBMS multicast session announcements, user authentication and authorization, and signaling. In order to support MBMS services all UMTS network elements require additional functionality.

MBMS multicast data distribution is designed only for downstream connections (from the BM-SC to the UE); any upstream multicast traffic must go to the GGSN and then forwarded to the intended recipients. Multicast group joining and leaving is carried out through IGMP messages and multicast groups are represented by IPv4 class D addresses. MBMS is designed for IP multicast interoperability. However, the interface that connects the BM-SC to external Packet Data Networks (PDNs) is not yet specified in the latest 3GPP release. Therefore, MBMS services are limited to a single UMTS network.

3. Related Work

Research proposals regarding AAA in IP multicast typically follow one of two approaches: the modification of IGMP/MLD signaling or the introduction of intermediate control layer between IP and IGMP processing.

The first approach requires the modification of multicasts group management protocols (IGMP and/or MLD) in order to carry user authentication information. In [13] and [14], the authors modify IGMPv3 to contain user credentials or digital certificates. The architecture detailed in [10] makes use of a previous IGMPv2 modification proposal [12]. These solutions follow the general AAA architecture as defined in [19] but applied to multicast sessions, meaning that the Network Access Server (NAS), upon receiving a IGMP join request, uses the authentication information contained within the IGMP packet to send an authorization request to an AAA server in order to verify the users rights to access the intended IP multicast stream.

The second approach consists in introducing an intermediate control layer between IP and IGMP processing. An example of this type of solution is presented in [18], where the authors propose a new communication protocol referred to as Multicast Control Protocol (MCOP), used to exchange messages between the edge router and the Multicast Controlling Agent (MCA). The MCA is responsible for multicast sessions access validation based on IP addresses within the IP/IGMP packets. This type of solution still requires some changes to network equipments to add multicast AAA. Since no protocol modification is required, it should be easier to implement it than solutions demanding IGMP modifications.

In [17] the authors suggest a portal-based system where a user, in order to receive a multicast stream, would authenticate himself on a web portal and then, after a successful authentication, an entity called NetWrapper would configure the edge device to enable multicast distribution. No men-

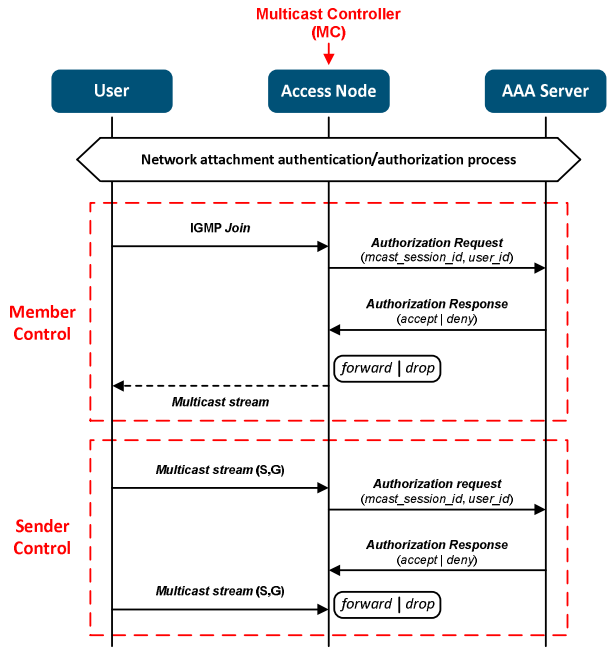

Figure 5. IP Multicast access control process

tion is made on how IGMP messages fit in their scheme or how would the portal retrieve information regarding the edge device associated with the request.

Work related to IP multicast AAA is also being carried out within the IETF MBONE workgroup. In [9] the requirements for multicast AAA (including QoS related issues) are undergoing specification, and in [21] a general multicast AAA framework is being designed to address similar requirements.

4. Proposed Solution

The solution proposed in this paper, for sender and receiver multicast access control, is shown in Figure 5. It consists of a new functional block, the Multicast Controller (MC), which is added to existing access nodes. The MC is responsible for the detection of multicast sessions, be it an IGMP packet (receiver control) or a multicast data stream (sender control), and the subsequent authorization request to an AAA server. The authorization requests sent by MC (RADIUS or DIAMETER messages) contain the user and multicast session identifiers that are obtained from the available network information at the access node (e.g. IP address, and line ID). Upon a successful authorization, the IGMP packet (receivers case), or the multicast stream (senders case), is processed normally by the access node. In case of an unauthorized access, the packets are discarded before they reach the IP layer at the access node.

Received Packet	Multicast Session IDs
IGMPv1/v2	SA, GDA
IGMPv3	SA, GDA, GSA
UDP multicast	SA, DA

Table 1. Multicast session IDs source

In order to exert sender and receiver multicast IP control at the access node, the MC must be able to uniquely identify the multicast session and authenticate its user. Table 1 summarizes the multicast session identifiers adopted, which are obtained directly from multicast IP packets. A members session can be identified in one of two ways, depending on whether IGMPv1/v2 or IGMPv3 is used. In the case of IGMPv1/v2, the members session is identified by the users IP Source Address (SA) and the Group Destination Address (GDA). In case of IGMPv3, along with the SA and GDA, a third identifier is also used, the Group Source Address (GSA). The SA is the users IP address; the GDA is the groups IP address the user wants to join or is currently a member of; the GSA is the IP address of the multicast groups source.

In the access networks considered, a successful network attachment is subjected to a valid user authentication. This process allows network operators to register network parameters associated with each connection, such as the users IP address. Since these network parameters are available to the access node, it enables this network element to identify a previously authenticated user. In order for the AAA server to determine whether a user can access a certain multicast group, or can transmit packets, it must have access to the multicast profile associated with this user. This profile contains the users information pertaining IP multicast data transmission and reception rights.

To improve the overall system performance and minimize authorization requests, the MC should keep a temporary white list of previously authorized multicast sessions, and translate that list into access control rules. In this way, packets belonging to previously authorized sessions are immediately accepted, eliminating the delay associated with the inclusion of the MCs functionality at the access node. This is especially critical for multicast sources, where the multicast stream can have a high bit rate and any delay can have a direct influence in the video stream quality. The same principle applies for keeping a blacklist of recently unauthorized multicast sessions.

In Figure 5 we assume that the last multicast replication point is the access node. However, in case of L2 multicast replication, multicast forwarding must also be controlled at the last replication point. Either directly, by implementing a MC for L2 multicast, or indirectly by means of a level 2 control protocol, such as those defined in [20] and [22].

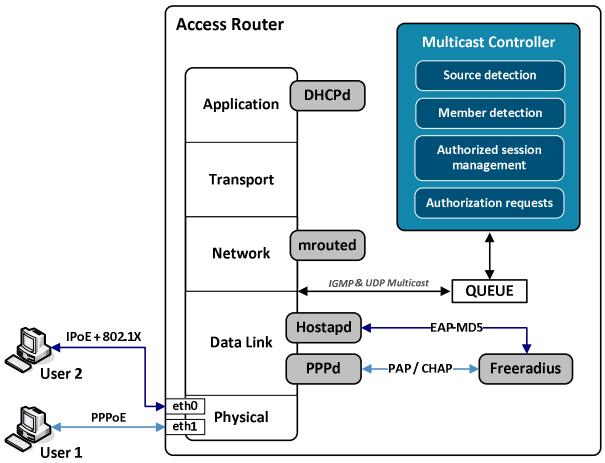

Figure 6. Prototype's functional architecture

5. Experimental Results

In order to verify the basic functionalities of the proposed solution, a prototype MC daemon was developed and implemented in a testbed consisting of 3 computers (Figure 6). One computer acted both as Access Node/Router (AR) and AAA server. The other two acted as users machines, each having a different connection type, PPPoE and 802.1X. The main functionalities identified were the following: user authentication; detection of join/leave messages; detection of multicast source transmission; multicast authorization permission checks; and unauthorized multicast traffic filtering.

Tests were executed to verify both the behavior and the performance of the MC. The first type of tests focused on the functional validation of the proposed solution, which included the system basic connectivity and the MCs behavior in the following use cases: authorized/unauthorized group join request; multicast transmission to an authorized/unauthorized multicast group; and unauthorize a source/member after transmission/reception has already begun.

In these tests one user acted as a source and the other as the receiver (group member). All the tests were successfully concluded, meaning that users were correctly authenticated on network attachment, and only when their respective access permissions allowed them they could access or transmit multicast content.

The second type of tests aimed at evaluating the performance of the proposed solution. In this case, the two users repeatedly sent IGMP join requests, at the highest rate possible, towards the AR. Small modifications were made to the MC so it would always process the join request. The MCs maximum processing rate was 1250 IGMP requests per second.

6. Conclusions

In this paper we identified the network elements where multicast receiver and sender admission control can be enforced, when considering multicast session spawning over heterogeneous access networks, namely, xDSL, WiMAX and UMTS. A prototype of the proposed solution was developed and functional and performance tests were carried out.

The proposed solution functions at the IP network layer, which makes it adaptable to all access networks considered. However, if L2 multicast replication exists, then the control over the last multicast replication point should also be implemented. Furthermore, some limitations exist, which are related to the various network architectures. In xDSL or WiMAX, a single connection can represent several users, which implies that the access control is performed on a per connection basis and not on a per user basis. In UMTS networks there are two possible scenarios, one with MBMS and another with typical IP Multicast. With the latter no sharing gains are obtained but the proposed solution can be fully supported. With MBMS, although multicast control is achieved, no users as multicast sources are supported.

The solution proposed in this paper does not require changes to user equipment or multicast protocols which facilitates the introduction of controlled IP multicast.

References

[1] 3GPP. Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (release 7). TS 23.246, 3rd Generation Parnership Proejct (3GPP), Sept. 2007.

[2] 3GPP. Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) (Release 7). TS 29.061, 3rd Generation Parnership Proejct (3GPP), Mar. 2008.

[3] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan. Internet Group Management Protocol, Version 3. RFC 3376 (Proposed Standard), Oct. 2002. Updated by RFC 4604.

[4] M. Christensen, K. Kimball, and F. Solensky. Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches. RFC 4541 (Informational), May 2006.

[5] A. Cohen and E. Shrum. Migration to ethernet-based dsl aggregation. *DSL Forum TR-101, May*, 2006.

[6] S. Deering. Host extensions for IP multicasting. RFC 1112 (Standard), Aug. 1989. Updated by RFC 2236.

[7] C. Diot, B. Levine, B. Lyles, H. Kassem, and D. Balensiefen. Deployment issues for the ip multicast service and architecture. *Network, IEEE*, 14:78–88, 2000.

[8] B. Fenner, H. He, B. Haberman, and H. Sandick. Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding

(IGMP/MLD Proxying). RFC 4605 (Proposed Standard), Aug. 2006.

[9] T. Hayashi, H. He, H. Satou, H. Ohta, and S. Vaidya. Requirements for multicast aaa coordinated between content provider(s) and network service provider(s). *draft-ietf-mboned-maccnt-req-05.txt*, Sept. 2007.

[10] Y. Hinard, H. Bettahar, Y. Challal, and A. Bouabdallah. Aaa based security architecture for multicast content distribution. *Computer Networks, 2006 International Symposium on*, pages 85–90, 2006.

[11] IEEE Std 802.16-2004. IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 2004.

[12] N. Ishikawa, N. Yamanouchi, and O. Takahashi. An architecture for user authentication of ip multicast and its implementation. *Internet Workshop, 1999. IWS 99*, pages 81–87, 1999.

[13] S. Islam and J. W. Atwood. A framework to add aaa functionalities in ip multicast. *Telecommunications, 2006. AICT-ICIW'06. International Conference on Internet and Web Applications and Services/Advanced International Conference on*, pages 58–58, 2006.

[14] S. Islam and J. W. Atwood. The internet group management protocol with access control (igmp-ac). *Proceedings of the 31st IEEE Conference on Local Computer Networks (LCN 2006)*, 2006.

[15] H. Jeon. Transmission of ip over ethernet over ieee 802.16 networks. *draft-ietf-16ng-ip-over-ethernet-over-802.16-02 (work in progress), July*, 2007.

[16] P. Judge and M. Ammar. Security issues and solutions in multicast content distribution: a survey. *Network, IEEE*, 17:30–36, 2003.

[17] O. Karppinen, O. Alanen, and T. Hamalainen. Multicast access control concept for xdsl-customers. *Consumer Communications and Networking Conference, 2006. CCNC 2006. 2006 3rd IEEE*, 1, 2006.

[18] R. Lehtonen and J. Harju. Controlled multicast framework. *Local Computer Networks, 2002. Proceedings. LCN 2002. 27th Annual IEEE Conference on*, pages 565–571, 2002.

[19] C. Metz. Aaa protocols: authentication, authorization, and accounting for the internet. *Internet Computing, IEEE*, 3:75–79, 1999.

[20] S. Ooghe. Framework and requirements for an access node control mechanism in broadband multi-service networks. *draft-ietf-ancp-framework-06 (work in progress), May*, 2008.

[21] H. Satou, H. Ohta, C. Jacquenet, T. Hayashi, and H. He. Aaa framework for multicasting. *draft-ietf-mboned-multiaaa-framework-06.txt*, Feb. 2008.

[22] S. Wadhwa and J. Moisand. Protocol for access node control mechanism in broadband networks. *draft-ietf-ancp-protocol-02 (work in progress), May*, 2008.

[23] WiMAX Forum NWG. WiMAX Forum Network Architecture Stage 2-3. Release 1, Version 1.2, 2008.