Multicast Access Control Concept for xDSL-customers

Olli Karppinen, Olli Alanen and Timo Hämäläinen
Department of Mathematical Information Technology
40014 University of Jyväskylä, Finland
{ollkarp, opalanen, timoh}@cc.jyu.fi

***Abstract*— Multicast is a tempting possibility for many broadband services. It makes possible to deliver one data-stream to several receivers simultaneously. IP-Multicast is based on an open group concept. This means that it is possible for all the users to join the group and thus receive the data. The open concept is also the main reason why multicast has not been taken in wider use. There is two different solution to solve this problem, group access control and multicast data encryption. Group access control mechanisms focuses on restricting the group membership at the users edge device. Traffic encryption scheme relies on end-to-end encryption, so a key management architecture is also needed. We introduce our own proposal for a multicast group access control mechanism. Our mechanism consists of user authentication and dynamic access control list configuration. Our proposal is protocol independent and thus easy to take in use in various content delivery network environments.**

I. Introduction

IP-Multicast is the only way to transfer one data-stream to multiple receivers simultaneously [3]. This is especially usefull with applications like IPTV, video - and audio conferences and other group communications. The idea behind the technique is to construct a delivery tree between the senders and the receivers and then forward the stream through the branches of the tree. This way, multicast saves bandwidth and processing power from the routers, who have to forward the stream only once on each link. Multicast is based on open group memberships, which means that anyone can join to group and receive the stream. Anyone can also send to the group, which enables many-to-many communications.

IP-Multicast has not reached the popularity that was predicted. The reason for this is the uncontrollability of the technique. The open membership is a benefit and a weakness at the same time. Especially for the commercial purposes, more control is needed to achieve the trust and controllability that the service providers want. Providing a liable television broadcast is an example of application that could be transferred using multicast, but then the membership can not be open. Some kind of authentication, authorization and accounting scheme must be implemented to achieve the control of the content. An external admission and access control is therefore needed.

Another aspect on the need for an admission control is Quality of Service (*QoS*). Differentiated Services (*DiffServ*) and multicast are not currently applicable on the same network because of some imcompatible features. These conflicts must be solved and some of them can be solved by using a proper admission control mechanism. Our previous works [1], [2] concentrated on the QoS-based admission control. In these papers, two measurement-based and one parameter-based methods were presented. The methods keep the QoS of existing customers as demanded, by rejecting some of the join requests. The decision is done based on either QoS measurements or calculations. The methods were simulated with ns2 simulator and good results were gotten.

The problems with the open membership can be solved with two different ways. The first one is to encrypt the multicast data and deliver the decryption key only to the allowed receivers. The second solution is to deliver the content only to the allowed receivers. A combination of both of them is also possible. Our approach is based on the idea that current multicast protocols will be used and the mechanism must be usable without any modification to the routers of the network. We have implemented our method to be used in a pilot network where IPTV is delivered to the customers behind the xDSL connections.

The general framework for our study is the model of the content delivery network. The framework is described in figure 1. This framework specifies different entities of multicast content delivery network. One entity is the content service provider controlling the content servers. Another entity is the network service provider offering the network infrastructure and the connections. As third entity are the customers receiving the service.

The rest of this paper is organized as follows. Chapter 2 introduces the basic concepts behind this work and the previous suggestions to solve the problem. In chapter 3, is our solution presented and chapter 4 describes the conclusion and further scenarios of our study.

II. CONTROLLING AND SECURING THE MULTICAST CONTENT

The entity of controlling and securing the multicast content consists of two main parts: multicast receiver access control mechanism and multicast traffic encryption. Receiver access control is mainly securing the multicast group from undesired members and thus protecting the content. Access control mechanisms are also used to protect the networks from Denial of Service problems, but traffic encryption has been used to ensure that only the legal receivers can benefit from the

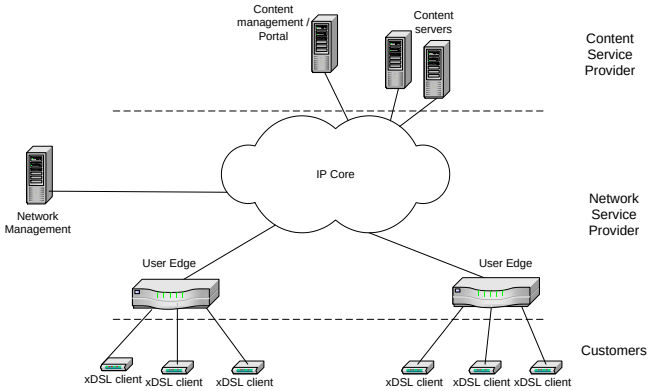

Fig. 1. The framework for the multicast content delivery network.

multicasted traffic. These two blocks together build up a controlled multicasting concept, in which both the network resources and the content can remain safe.

There are some general functional requirements that can be settled for all multicast receiver access control mechanisms. One of the most important issue is user authentication mechanism. User authentication has to be performed before any other access control function can be executed. Authentication is very closely related to another important access control function, user authorization. Authorization means ensuring the users rights to the requested service. Third important requirement for receiver access control mechamism is its compatibility with the present forwarding system, which can be e.g controlling the access lists.

While multicast group membership is open and dynamic, the most efficient way to protect the content is to encrypt it. Encrypting basically means that the data (e.g IPTV-stream) will be encrypted at the sender end and decrypted at the receivers end. Cryptographic operations are performed by using so called group key, which means that the same key is shared among all group members. Group key is delivered only to legitimated (autheticated, authorizated) receivers who thus are able to get the content. Traffic encryption schemes thus meet the same requirements of authentication and authorization than group membership access control mechamisms.

There is often also a need for management for the multicast source. This is where the source specific multicast -model will be the key factor. In this study we focus only on one to many -multicast model with one sender and multiple receivers. [4]

A. Multicast Receiver Access Control Solutions

Multicast receiver access control mechanisms can be divided in two basic categories by the ways they handle the problems of multicasting. Our divisioning is based on the modifications done in the current multicast protocol architecture. One often proposed approach is to extend the group management protocols by adding access control functionality. In [7] the authors propose a method for user authentication and group access control in IP multicast. Their method is based on extended IGMPv2 running at senders and receivers edge device. They have added new fields in IGMPv2 for transporting the authentication data. Edge devices communicate with a RADIUS -server to authenticate the multicast senders and receivers. Based on the authentication result, the ingress and egress routers either accept the clients to the group or reject them. In [6] the authors propose a user authentication and access control mechanism based on IGMPv3. In their method the receivers edge routers act as local controllers. These elements communicate with one global controller. Authentication is based on token-field attached in IGMPv3-packet. All receiver information is saved in external directory server, which acts as a authentication server. Token-field is also protected by receivers private key. This model also includes the possibility to deliver the channel key needed to decrypt the encrypted content. The usability and wide commissioning in real life situations is the biggest difficulty of these extended group management protocols. Large scale replacement of the current protocol architecture is not likely to happen.

Another aspect of constructing the access control is that the current group management protocols remain unchanged and a new layer for the access control is implemented. The layer can be set below the group management protocol, so it will operate like a filter layer. An example of this kind of architecture is introduced in [5]. The authors have defined a multicast control protocol, which blocks join-messages sent by unlegalized clients. Architecture framework consists of aMulticast Control Protocol (MCOP)-capable router and an external multicast control agent. Multicast control agent acts like a database and updates the current client information to the MCOP-router which can filter all unlegalized joins and thus prevent those illegal clients to join the group. This kind of separated control protocol -layer is a little bit easier to take in real life use, while it does not set any specific requirements on the software of the multicast clients.

Both of those aspects set requirements for modifications in the current multicast architecture. It means that commissioning in real world and commercial use is quite difficult. Third possibility is to construct completely extrenal access control architecture. By doing so we achieve a protocol independent mechanism, which will be easy to implement and first of all easy to take in real life use. External solutions also scale and work better alongside with new network protocols and techniques to be taken in use in near future. We have based our own access control mechanism in this external aspect.

B. Multicast Traffic Encryption Solutions

The traffic encryption is another aspect of the multicast content management. Encryption is usually performed by using so called group key, which means that the same cryptographic secret is shared among the senders and the receivers. Traffic encryption is basically quite simple operation,but the problem that arises is the re-keying and group key management. Re-keying means the regeneration and re-distributing the new keys to the clients. It has to be done always when a group member leaves a group and it might be necessary also when a new user

joins the group. Group key management includes thus creating, possessing and distributing the keys to the group members.

Traditional ways like smart cards are not very flexible in dynamic multicast commnunications. There is a need for flexible and scalable group key management architecture. Scalability is very important requirement especially in the cases of very large groups.

Basically, group key management schemes can be divided in centralized and distributed models. In centralized model there is one group controller in the network that takes care of generating and delivering of the group keys. Centralized model does not scale very well in re-keying when the group size is big. Basic example of centralized is defined in [8]. In distributed key management architectures the responsibility of key delivery is divided to several key distribution centers. Thus the scalability is usually better in distributed architectures. One definition of distributed approach is defined in [9].

III. Practical Tests and Implementation issues

Our main motivation on creating a new access control scheme was to make it work in current networks with current protocols. The edge nodes of our test network are DSLAMs and routers work as core nodes. Customers have IP Set-top-boxes as host devices. This particular topology made it impossible to use some router specific features. Our approach is scalable, secure and highly dynamical. It also takes care of the mobility of xDSL-customers. Authentication and access control functions can be performed regardless of the physical location. For this functionality we have specified an id for all xDSL-clients participating in IPTV content delivery network. Broadband id consists of DSLAM's IP address and customers port number, which together are correspond to one id-number. By using this broadband id and mobile phone it is possible for customer to subscribe the IPTV-service also elsewhere than home. The idea behind our access control model is to use existing technologies and combine them with each other. The glue between the components, is a network management entity called NetWrapper [10]. It configures the network devices to control the access to the contents.

Our model also makes accounting easy in differnet kind of accounting schemes. Three different accounting models were considered in our model. First group of content is free, where no authentication nor accounting information is needed. The second one is a fixed-term access, where customer has payed eg. a monthly fee and where the access must be controlled, but no accounting information needs to be stored. The third and final one is a pay-per-view model where the accounting is done in a time-based manner and both the access control and accounting information has to be handled.

A. Access control components

The access control mechanism of our content delivery network consists of four essential component. Proposed access control mechanisms topology and functionality is described in figure 2.

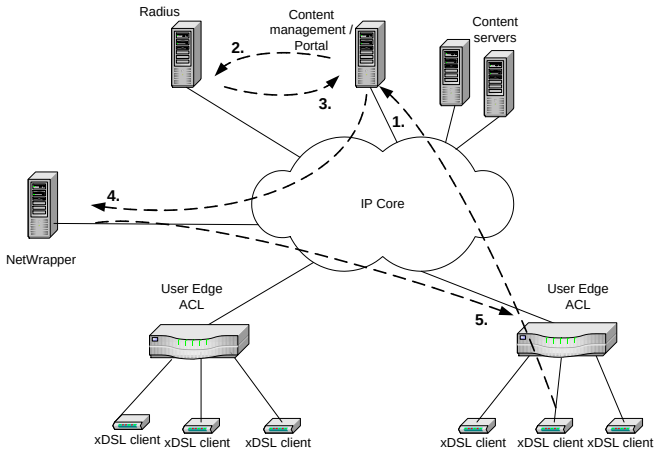

Fig. 2. Controlled content delivery model.

Service portal is a central component of our model. It's the place where the customer can choose the service he/she wants to start receiving. The portal is separated from the content servers and used as a service management unit. Portal server also communicates with the Radius server to authenticate the users when a restricted service is selected so it thus operates as a NAS-client. NAS (network Access Server) is the entity that sends the authentication requests to Radius and receives the acknowledgements.

Radius is used to save the user authentication data and to collect the accounting information. We have configured our Radius to support some extra attributes. We have also combined an extended version of Radius-server in our access control architecture. This server communicates with sms-gateway and is able to handle the mobility of the users. It uses one-time passwords and challenge-response authentication.

Access control list is used to allow or deny the receiving of multicast traffic at the users edge device. We have digital subscriber line access multiplexer (DSLAM) as our edge device. Our access control list has the property to allow or deny the client to join to the multicast channel, basing on the xDSL clients edge device -port. A port can be permitted to receive only one multicast channel or a bunch of channels.

NetWrapper is a network management entity that combines the Radius authentication and the access control list modifications to become a functional entity. Practically it performs the crucial network device configurations dynamically, which helps us to minimize the amount of manual work. NetWrapper is able to perform configurations in diverse network elements. In our model NetWrapper performs the access list configurations via Telnet-connection.

B. Access Control Process

One of the most important tasks in every access control mechamism is the user authentication. Our model performs the user authentication when the user selects a restricted service at the portal (message 1 in figure 2). Portal operating as a NAS-client sends an access request to the Radius server (message

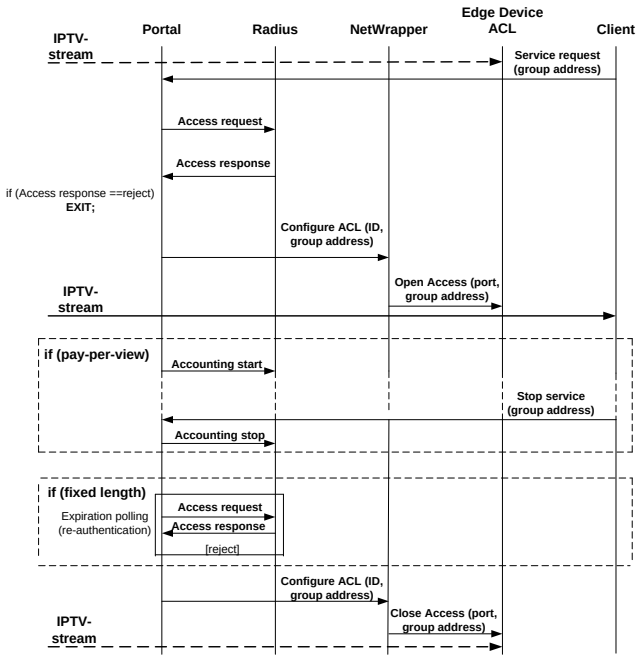

Fig. 3. Sequence diagram of our access control and accounting models.

2). Radius authenticates and authorizates the user and replies either accept or reject as a response (message 3).

When the customer wants to utilize the xDSL-technology to receive multicast-IPTV somewhere else than home, he can perform the authentication by using the extended version of Radius. For this purpose he has to input his mobile phone number as username and broadband id for his current position at the content delivery network. He will receive one-time password in SMS in his mobile phone and perform then the challenge-response authentication with this password. This mechanism is also possible by utilizing the existing technology.

Next phase of the access control process is executed when the user authentication and authorization is successfully done. Portal receives the acknowledgement from the Radius. Portal then dynamically sends a command to NetWrapper to configure the edge devices access control list to enable the multicast client to join the group and receive the IPTV-stream (messages 4 and 5). These commands include users edge device port and desired multicast channel address as parameters. When it is the case of mobile customer, the command that portal sends to the NetWrapper consists of broadband id and preferred IPTV multicast service. Sequence diagram of our access control mechanism and accountig features related to it are described in figure 3.

C. Accounting schemes and re-authentication

Our access control architecture enables also two different models to take care of the accounting. It is possible to use both fixed length subscriptions and pay-per-view accounting. Both of them are handled by using features of portal and Radius servers. When the fixed length subscription is in use, it is also necessary to take care of the re-authentication of the user during the service.

Fixed-term subscriptions are managed by configuring the Expiration-attribute of Radius to match the desired period. When the user is trying join the group after the subscription period is over, Radius sends an access reject message. At this point NAS commands NetWrapper to configure the ACL to deny the receiving the service that expired. If the customer does not cut off the multicast stream at any point of the subscription period, it is possible to continue the reception of the multicast after the subscription is over. To prevent this kind of illegal reception of the service, re-authentication has to be done. Our re-authentication means that messages 2, 3 (and 4) in figure 2 are executed in desired interval, e.g once in an hour. If the subscription period is over, Radius sends an access reject and thus the NetWrapper closes the access to the service.

Pay-per-view -accounting is managed by using the accounting features of Radius. When a user starts to receive a pay-per-view -service, an accounting start -message is sent to the Radius. When the user stops receiving the service, portal sends an accounting stop message to the Radius. The accounting management can be handled e.g by an external application at Radius. Re-authentication functionality is not needed in pay-per-view -services, because the user decides how long to receive and pay for the service. Possible damage caused by Radius message losses is noticed by setting up a retransmission timers in the NAS. Our model also enables the use of parallel Radius AAA-servers simultaneously, which improves the reliability of our model.

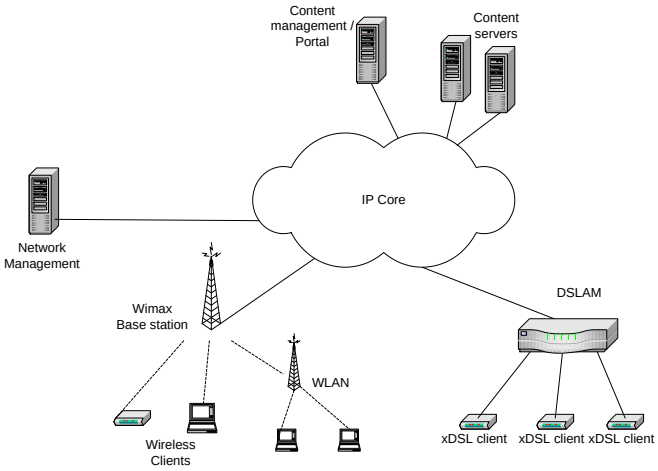

Fig. 4. Heterogeneous access network.

IV. CONCLUSIONS

In this paper, we have porposed a new admission control mechanism to control the receiving of multicast content. Our method is already implemented and does not need any changes to the current multicast or any other protocols. We have tested it in a xDSL pilot network, where the control of eg. IPTV services was handled with our method. It is also a secure

solution, thus the only requirement is to have correct user information in Radius server.

We will continue the development of this method and at least some QoS measurements will be added to the method. Then the customer will be joined to the group only if authrorized and the QoS constraints may be satisfied. We will also pay attention to the wireless multicast and its access control issues. At least WLAN and Wimax will be examined. Proposed framework for our future examinations is specified in figure 4 .

REFERENCES

[1] Alanen O., Pääkkönen M., Ketola M., Hämäläinen T., and Joutsensalo J.,"Enhanced Admission Control Solution for Multicasting With DiffServ", 1st Conference on Next Generation Internet Networks, 2005.

[2] Alanen O., Pääkkönen M., Hämäläinen T., Ketola M., Joutsensalo J., "Measurement-Based Multicast Admission Control in DiffServ Networks", 7th International Conference on Advanced Communication Technology, 2005.

[3] Deering S.,"Host Extension for IP Multicasting, RFC 1112".

[4] Judge P., Ammar M., "Security issues and solutions in multicast content distribution: a Survey". Network, IEEE , Volume: 17 , Issue: 1, Jan.-Feb. 2003.

[5] Lehtonen R., Harju J., "Controlled multicast framework", 27th Annual IEEE Conference on Local Computer Networks, 2002., 6-8 Nov. 2002.

[6] Chaddoud G., Varadharajan V., "Efficient secure group management for SSM" , IEEE International Conference on Comminications 2004, Volume: 3, 20-24 June 2004.

[7] Ishikawa N., Yamanouchi N., Takahashi O., "An Architecture for User Authentication of IP Multicast and Its Implementation", IEEE Internet Workshop 18.-20. February 1999.

[8] Harney H., Muckenhirn C., "Group Key Management Protocol (GKMP) Architecture, RFC 2094".

[9] Ballardie A., "Scalable Multicast Key Distribution, RFC 1949".

[10] WTS Wireless systems ltd., Available at <URL:http://www.wts.fi>, 25.2.2005.