Authentication, authorisation and accounting in distributed multimedia content delivery system.

Mirosław Czyrnek, Marcin Luboński, Cezary Mazurek

Poznań Supercomputing and Networking Center (PSNC),
ul. Noskowskiego 10, 61-704 Poznań, Poland

phone: +48 61 858 20 30, fax: +48 61 852 59 54
e-mail:{majrek, laser, mazurek}@man.poznan.pl

Keywords: streaming, content delivery, middleware

Abstract

The paper describes the solutions to the authentication, authorisation and accounting (AAA) problems in a distributed multimedia content delivery system. It summarises the effects of works, which have been conducted in PSNC for over a year now to develop an efficient and reliable multimedia distribution middleware platform. The paper focuses on the part of the system's functionality which limits access to the digital content only to the authenticated and authorised users, and presents a distributed accounting system.

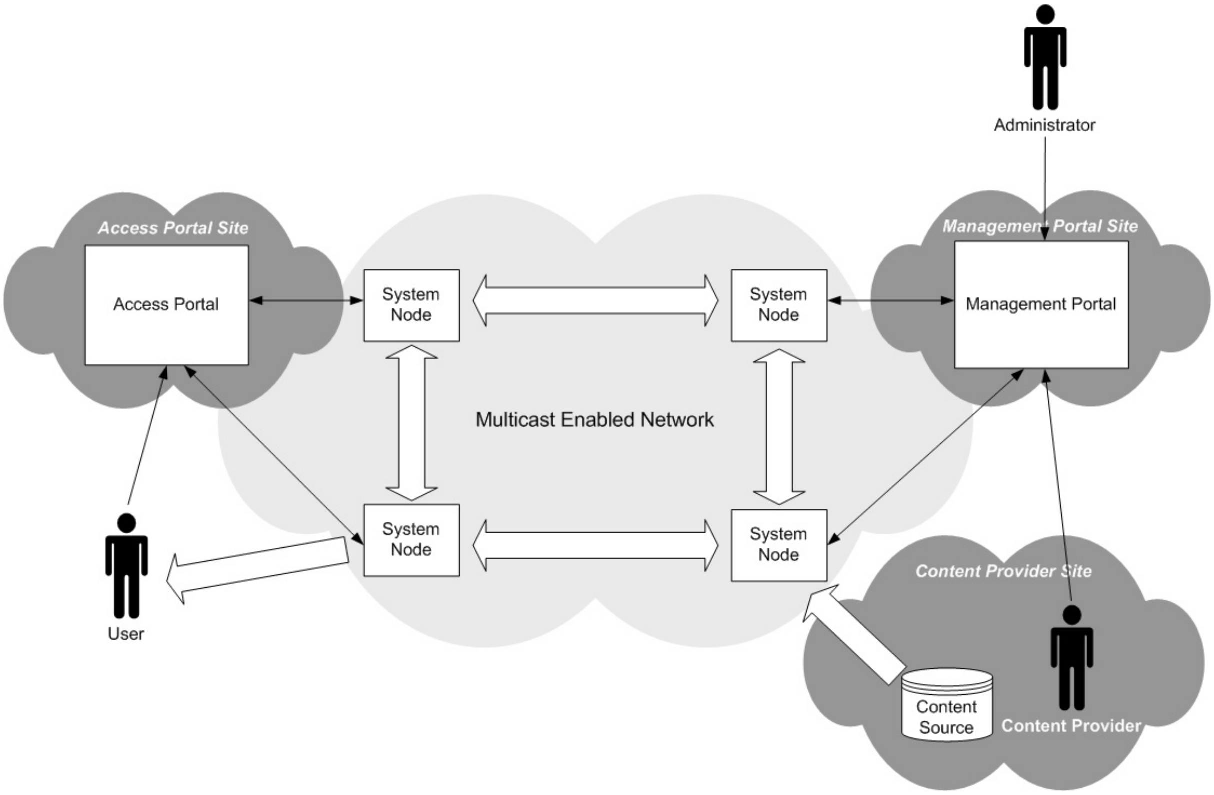
Conference subject area: ACCESS **-** Authentication, Authorisation, and Accounting (AAA), mobility, last mile, resources discovery, firewalls and wireless networking, digital rights management, copyright and accessibility

Introduction

The ubiquity of the digitalisation of the multimedia content has provided the means for easy but, unfortunately, frequently uncontrolled content distribution. The streaming technologies seem to be a solution to the problem of illegal copying, so that wide deployment of services such as interactive TV or video on-demand is possible. However, without dedicated procedures of authentication and authorisation the content is vulnerable to illegal access.

The Content Delivery Systems (also known as Content Delivery Networks - CDNs) provide secure and scalable transportation of multimedia streaming content from the providers to the end-users. In order to assure high reliability and capacity to serve many users, CDNs are based on dedicated, homogeneous nodes distributed over the network, which makes the content closer to the user. Each node can perform splitting and caching functions for live and on-demand content delivery. Available CDN solutions focus on efficient content delivery rather than provision of unified access to the multimedia resources for the users as well as AAA procedures. Therefore, there is a need to provide an open, scalable and reliable solution that is able to support end-to-end multimedia delivery with a unified user access rights management, and deploy distributed AAA procedures.

The system, developed in PSNC benefits from the CDNs architecture defining distributed nodes that are able to split and cache multimedia content. According to grid concepts, it provides an advanced middleware layer that is responsible for content management and distribution, and allows integration of many vendor specific streaming media platforms. System components and actors are shown in Picture 1. Access portals are responsible for content presentation and users management. The middleware services, implemented in system nodes, in co-operation with access portals, are responsible for AAA procedures. The management portal allows many content providers to feed the system with content by building their own multimedia content catalogue and enables content distribution policy management. Every content provider has to register his own content sources in the system in order to point at where the content originates from.



Picture 1 - System components & actors

The innovation of the applied architecture focuses on transparent access to different multimedia resources via access portals as well as providing unified AAA procedures. Such an approach supports the content originating from many sources owned by various providers. The content can be published in the multiple access/end-users' portals and finally delivered to its clients with maxium multimedia experience to the end-user.

The proposed distributed system architecture along with a specific application of the system define several important requirements. The system must, by all possible means, ensure that access to the content will be restricted only to the authorised users. Moreover, any access limitations and procedures implemented in the system should not contradict the possibility of the system usage as a basis for the public and commercial content delivery service. The a*uthentication, authorisation* and *accounting* procedures have to take into account the distributed system architecture and the copyrights preservation but also have to support multiple business models that could be implemented by the content providers or access portals. Another very important issue is to make access to the content as transparent as possible, which must also be independent of the internal system organisation and the implemented procedures. It is similar to the grid approach in the area of providing unified computing resources access.

The proposed solutions to the problems and requirements concerning AAA are described in details further in this paper.

AAA in distributed multimedia content delivery system

According to the model of the services, which are provided by the system developed in PSNC, four main types of elements have been distinguished:

- *content source* – providing both on-demand and live multimedia streams from a particular content provider site

- *system nodes* - forming the core of the distribution system responsible for splitting and caching of multimedia content
- *management portal* – providing access to nodes and sources configuration as well as content management functionality for content providers
- *users'/access portals* – providing access to the content available in the system along with the metadata describing it

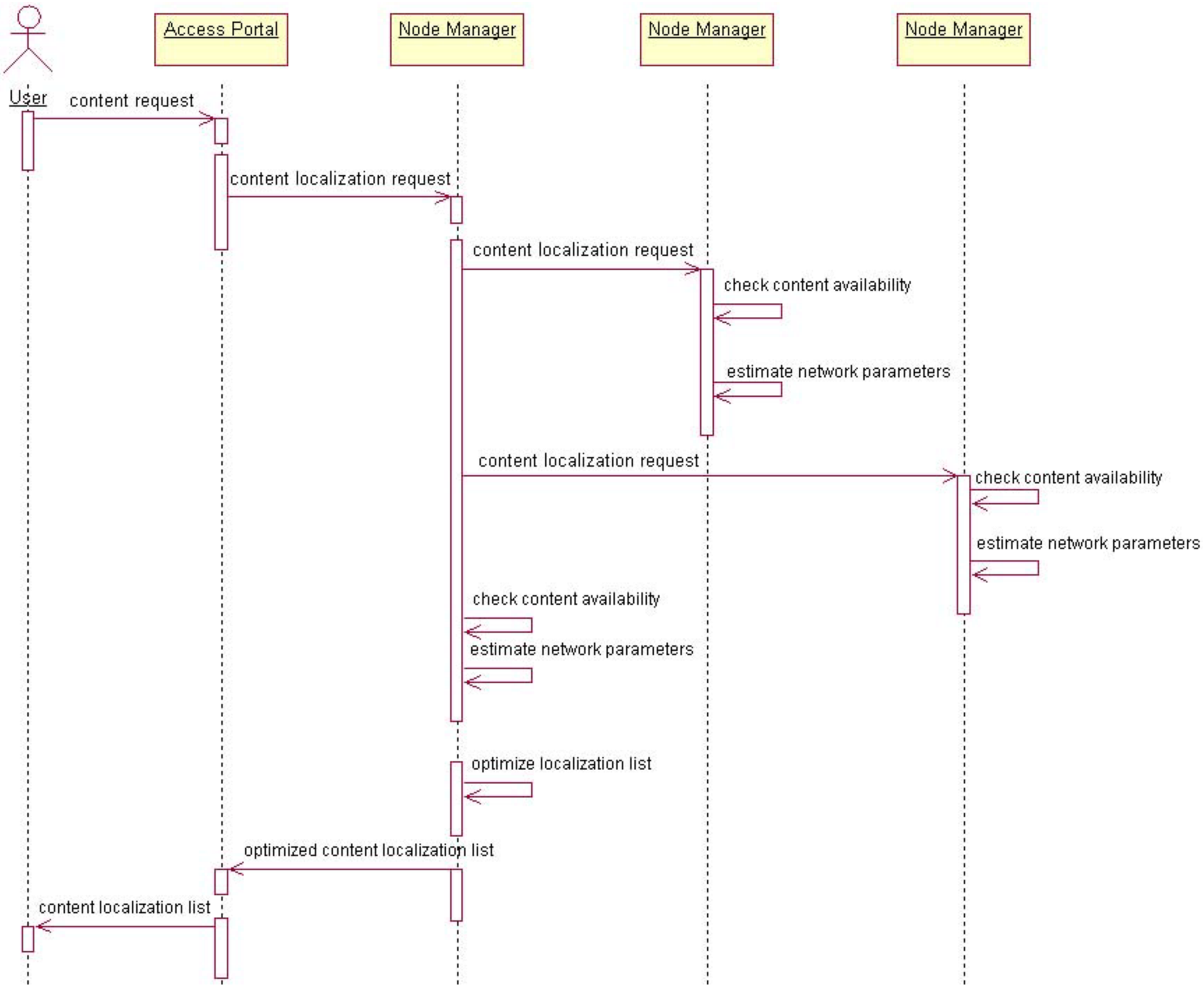
With respect to the system capabilities, including the definition of different policies of content distribution by each of the content providers and multiple access policies in the users' portals, it seems to be more reasonable to locate components responsible for AAA closer to the end-users. This makes them independent of any specific internal solutions and protocols. Therefore, all information required for authentication and authorisation of the end-users is stored in local databases of access portals. In a similar way all statistics on content usage are continuously gathered and stored in the portal where the user is registered. However, another accounting policy may be implemented in which the access portal requests accounting information from the system nodes. Accounting information may be used later as a basis for billing according to a suitable business model.

Implementation (of the AAA procedures)

The AAA procedures in the system are performed among the end-user, system nodes and the appropriate users' portal. The implementation of the AAA procedures in the distributed multimedia content delivery system requires that each of the mentioned elements should have specialised interfaces to provide the appropriate functionality.

The authentication and authorization as well as accounting procedures involve the same system components. The authentication and authorisation in the system node is performed separately from user authentication and authorization in the access portal and prior to serving user's content request. This ensures that every content request, which is directed to the streaming server, must be authorised, which prevents any illegal content access. Accounting procedures are performed by means of specialised streaming server plugins that are capable of communicating with a node manager component. Every event that occurs due to the user activity is stored in the system node database and is passed to the access portal for further processing.

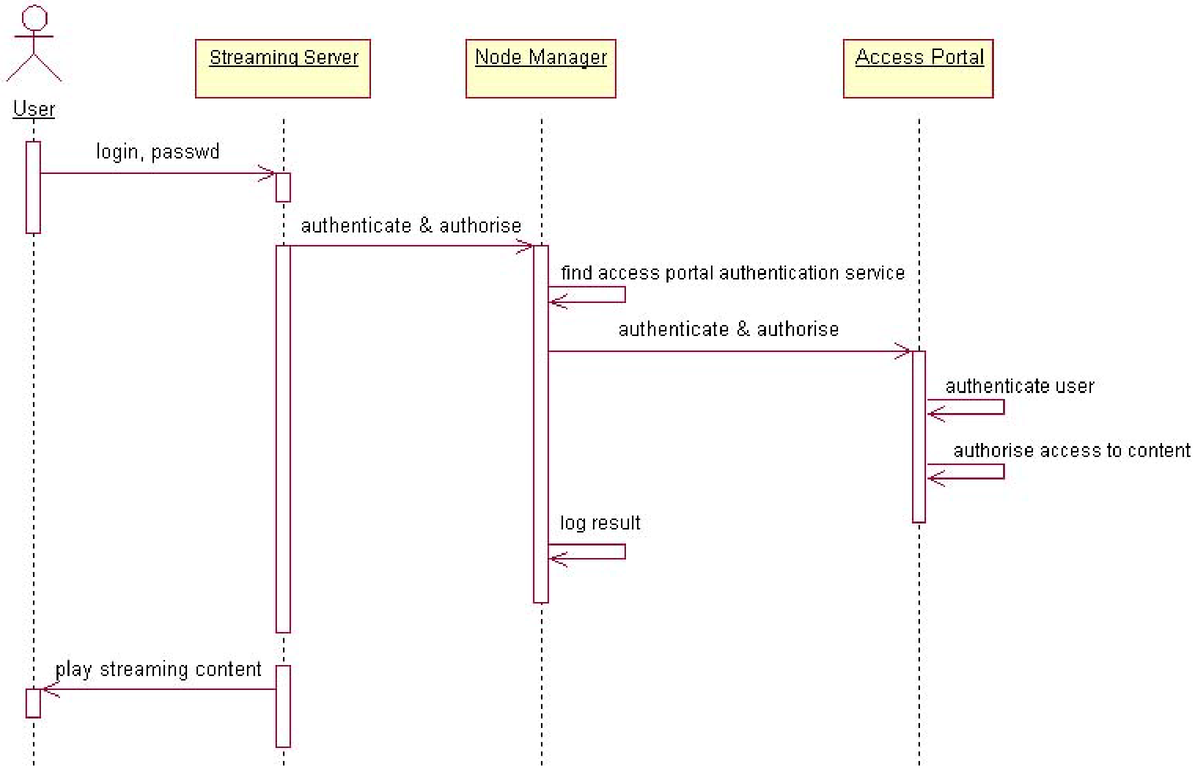
Procedures, which perform authentication and authorisation of the user in the corresponding users' portal, are invoked when the user content request is submitted to the access portal. The request initiates content localization in the system in order to determine the node that can provide the best quality of service. When content is requested, the access portal calls one of the node managers (this component is a part of each system node) in order to prepare a list of content localizations. The node manager asks other node managers to check the content availability in their nodes and to estimate network parameters in order to find optimized, that is for the best user experience and quality of service, content localizations. After this procedure the list of selected content localizations is returned to the user. The content localization procedure has been presented in Picture 2.


User
Access Portal
Node Manager
Node Manager
Node Manager
content request
content localization request
content localization request
check content availability
estimate network parameters
content localization request
check content availability
estimate network parameters
check content availability
estimate network parameters
optimize localization list
optimized content localization list
content localization list

Picture 2 - Content localization procedure (only three system nodes are depicted)

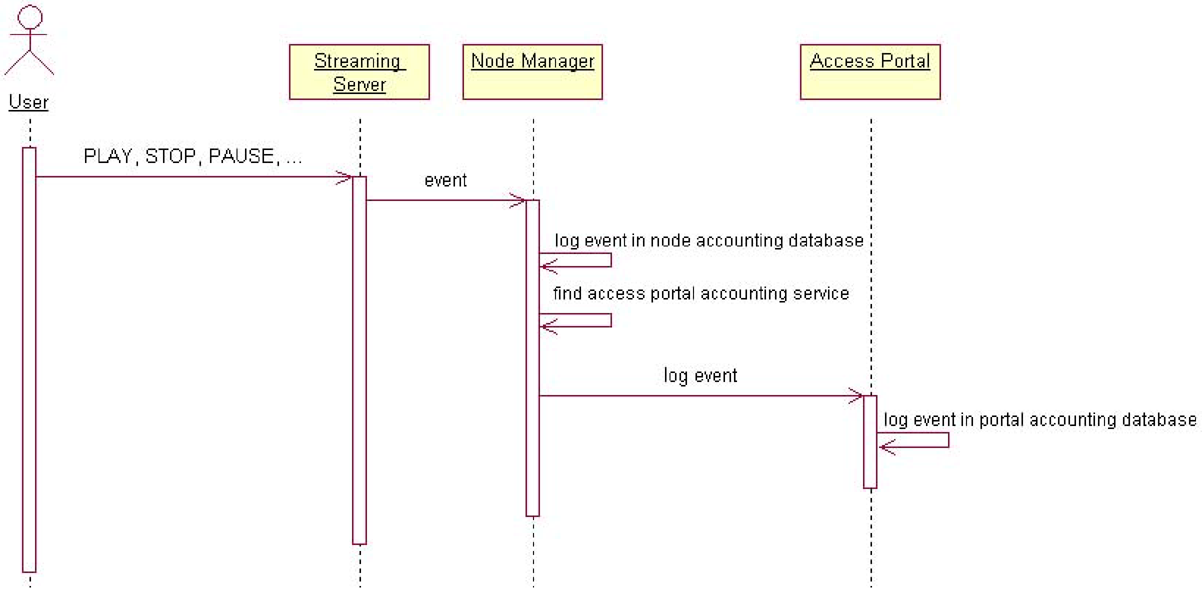
At the next stage, the user is directed to the streaming server in the best node. According to the approach taken in the design phase, the streaming server tries to authenticate and authorise the user request in the users' portal, because no user information is duplicated in the system node. To complete the procedure the streaming server must know the user login and password and the resource identifier, and has to identify the portal in which the authorisation can be performed. The latter two identifiers are passed along with the content request, while the former ones are provided by the user in the streaming player after successful content localization in the system. This prevents from passing complete information identifying the user and the portal where the user is registered in one message.

When the user requests the content from the streaming server, the server issues the authorisation request to the user. After completing the user/password form, user credentials are sent to the streaming server that tries to authenticate the user (see Picture 3). In order to do that, it calls the node manager that is responsible for passing the authentication request to an appropriate user's access portal. The access portal checks if the user's login and password are correct and validates user's access rights to the requested content. The result of this operation is returned to the streaming server. Passing the whole procedure successfully results in presenting the requested streaming content to the user.



Picture 3 - User authentication and authorisation

The procedure of gathering the accounting information starts when authentication and authorisation ends. Depending on the streaming server functionality in the system node, which regards tracing user events, a specialised component localized in the node stores statistics of the content usage locally. This data can be duplicated to the appropriate user’s portal every time the event (PLAY, PAUSE, STOP, ...) occurs. It can also be gathered in the batch mode on the request from the users’ portal, for instance to generate billing information for the users. Considering the first situation (see Picture 4) the complete information about the user activity in the nodes is consistent with the information in the user’s portal. In the second situation, however, the portal must send a request to every node, which has potentially gathered the required statistics and collect the fragments corresponding to the user.


User
Streaming Server
Node Manager
Access Portal
PLAY, STOP, PAUSE, ...
event
log event in node accounting database
find access portal accounting service
log event
log event in portal accounting database

Picture 4 - Accounting process

It is worth mentioning that every system component, prior to serving any internal request, performs authentication of the caller in order to provide services only for other system components.

Applied technologies

The modular organisation of the system provides maximum flexibility of the implemented solutions that enables easy modification and scaling. While the system components implementation is based on the Java and .NET technologies with JDBC database access, the SOAP protocol and WebServices technology is responsible for communication among all the system components.
The users' and management portals are both based on the Java Servlet and DHTML technologies. The system uses Microsoft Windows Media as the streaming platform, and as a result, the server plugins responsible for AAA are implemented as the COM components. But it is planned to support streaming media platforms provided by other vendors, which requires implementing specialised management interfaces that were developed by using vendor-specific SDKs.

Conclusions

The design of the described system benefits from the works in the area of grids and development of the applications for the Polish Optical Internet built within the confines of the PIONIER programme [1]. Therefore, the architecture of the distributed multimedia content delivery system has been designed to correspond with the organisation of the grid defined as a stack of fabric, connectivity, resource and application layers [2]. The system, similarly, has well defined elements like content sources located at content providers, distributed delivery system which is transparent for the end-users and based on the multicast-enabled IP network, and finally access portals presenting the content published in the system to the users.

Such system architecture requires that the AAA procedures should be independent of the particular implementation of the system structure and possible usage of different business models. Therefore, the whole responsibility for the authentication and authorisation decisions as well as the collection of the accounting information is held in the users' portals. Thanks to this approach there has been no need so far to bother about users data exchange and synchronisation among different portals and system nodes.

The system is still under development and its pilot version is used in the ATRIUM (IST-1999-20675) [3] project workpackage 5. The aim of this workpackage is to perform ATRIUM testbed experimentation and demonstration providing network-demanding applications. The test results will stimulate further works and verify the design decisions for the presented system.
In the area of AAA it is anticipated that the future works on the system will provide a solution to the problem of authentication and authorisation with respect to the end-user geographical location. Future works will also focus on the increasing of the internal system security in communication among WebServices components by the implementation of the HTTPS protocol for SOAP messages.

References

[1] PIONIER – Polish Optical Internet - http://www.pionier.gov.pl

[2] Ian Foster, Carl Kesselman, Steven Tuecke. The Anatomy of the Grid. Enabling Scalable Virtual Organizations. – http://www.globus.org/research/papers/anatomy.pdf

[3] ATRIUM IST-1999-20675 – http://world.alcatel.be/atrium

Vitae

Mirosław Czyrnek, born in 1978, received his Master's Degree in Computer Science from Poznan University of Technology in 2002. Since 1999 he has actively participated in works conducted in PSNC Network Services Department, concerning access portals and advanced network services. Since

2001 he has been involved in the development of multimedia content delivery system in order to provide interactive television services for Polish Optical Internet. Since 2002 he has been taking part in IST ATRIUM project and has been responsible for streaming media applications demonstration. His interests focus on advanced technologies appliances for the Information Society in the area of education and entertainment.

Marcin Luboński, born in 1978, has received his Bachelor's Degree in Computer Science in 2000 and in 2002 Master's Degree from Poznan University of Technology. He has been working for the Poznan Supercomputing and Networking Center since 1999. He participated in several development projects conducted in the Center concerning the design and implementation of the e-commerce portal framework as well as educational portals like the Polish Educational Portal – Interkl@sa. Currently he is working as a member of the team participating in the ATRIUM project. His main research interests include distributed systems, content delivery networks, streaming and caching technologies.

Cezary Mazurek, born in 1969, received his Master's Degree in Computer Science from the Poznan University of Technology in 1993. He worked for Poznan University of Technology between 1993 and 1994 and since 1993 he has been working for the Poznan Supercomputing and Networking Center (PSNC). He is currently the head of Network Services Department at PSNC. Since 1994 he has been a project leader of the international software project on designing and development of network testers' GUI, which is led in Poznan University of Technology. His interests focus on advanced network services' design and development, digital multimedia libraries, distance education systems and portal access to GRID services. He is co-author of an offer concerning advanced services for scientific users in the national POL-34/155 ATM network. The offer was presented during the POLMAN'99 conference and was rewarded by the National Committee for Scientific Research. He is author of many publications presented on national and international conferences. Since 1998 he has been organising annual presentation of advanced network services and applications developed by PSNC during the European Conference and Exhibition - Information Society Technologies.
Currently he is leading the development of services based on Internet technologies (e.g. Digital Library Framework: dLibra, Polish Educational Portal in co-operation with Interkl@sa, Multimedia City Guide in co-operation with Poznan City). Since December 2001 he has been a leader of the project "Creating an access environment for GRID computational services performed by cluster of SUNs", co-founded by the National Committee for Scientific Research and SUN Microsystems.