

Lightweight management of scalable and personalised media in mobile IPTV networks (Invited Paper)

Laura Arnaiz

Universidad Politécnica de Madrid
(GATV)
Av. Complutense, 30
Ciudad Universitaria, Madrid (Spain)
+34 91 549 57 00 ext: 8073
lav@gatv.ssr.upm.es

Lara García

Universidad Politécnica de Madrid
(GATV)
Av. Complutense, 30
Ciudad Universitaria, Madrid (Spain)
+34 91 549 57 00 ext: 8073
lgv@gatv.ssr.upm.es

Federico Álvarez

Universidad Politécnica de Madrid
(GATV)
Av. Complutense, 30
Ciudad Universitaria, Madrid (Spain)
+34 91 336 7344
fag@gatv.ssr.upm.es

José Manuel Menéndez

Universidad Politécnica de Madrid
(GATV)
Av. Complutense, 30
Ciudad Universitaria, Madrid (Spain)
+34 91 549 57 00 ext: 4072
jmm@gatv.ssr.upm.es

Guillermo Cisneros

Universidad Politécnica de Madrid
(GATV)
Av. Complutense, 30
Ciudad Universitaria, Madrid (Spain)
+34 91 336 7261
gcp@gatv.ssr.upm.es

ABSTRACT

In the present paper a novel system for scalable and personalised media management and its architecture is presented. The proposed solution is based on the creation of a secure and adaptable content delivery architecture and the underlying mechanisms to ensure the correct content management which, along with the content protection mechanisms, can be useful for, on one hand, ensuring user privacy and, on the other hand, enabling the possibility of offering commercial IPTV services over a mobile environment. The aim of the system is to enable personalised view, scalable, seamless and trusted multimedia content delivery, while protecting content from unauthorised access.

Categories and Subject Descriptors

C.2 [Computer-Communication Networks]: Miscellaneous.

General Terms

Management, security and experimentation.

Keywords

Mobile IPTV network, SVC, MVC, DRM, content protection.

1. INTRODUCTION

Widespread and affordable broadband access opens up opportunities for delivery of new streaming services. A change is expected in the way people use the network as, in few years, everyone will be multimedia content producer (by publishing digital pictures, video recordings, remote e-health services, home surveillance, etc.), multimedia content mediator (by

storing/forwarding streaming content) and multimedia content consumer (digital television, video on demand, mobile broadcasting and alike).

So it is important to offer the users adaptable and personalized contents through multiple kinds of networks and terminals [1]. One of the main coding technologies to offer both features is SVC (Scalable Video Coding) and MVC (Multi-view Video Coding) technologies.

For a commercial use and because of privacy issues when delivered over an overlay mobile P2P network, content should be properly protected to be able to be decoded uniquely by the targeted user. Adaptable and personalized contents over mobile P2P networks need special tailored content protection mechanisms which we will further describe in the paper.

In section 2, we describe the key technologies used in the proposed system. Later, in section 3, we present the system's architecture, with special emphasis in the content protection procedure. Finally, in section 4, we expose the conclusions obtained.

2. TECHNOLOGY PILLARS

In our work on personalized content protection for mobile P2P networks, we have found that there are several technology pillars that support the development of a successful content management system. These technology pillars are described deeply in the following subsections.

2.1 Multi-layered/multi-viewed content coding

For the proposed architecture we considered H.264 SVC and H.264 MVC as the major foreseen content delivery technologies over heterogeneous network. For this reason, one of

these technologies pillar is the Multi-layered/Multi-viewed content coding.

Scalable Video Coding (SVC) is a highly attractive solution to the problems posed by the characteristics of multi-networks, multi-sources, multimodal video transmission systems.

Multi-view Video Coding (MVC) addresses efficient integration of data and will provide for personalized views and extended 3D video functionalities.

Whereas SVC offers layered temporal/spatial/quality content scalability, MVC allows the user to select among the different views embedded in a single video stream.

These two technologies give the end users a truly personalized video delivery experience, by choosing the suitable content quality for his/her terminal and allowing the end user to interactively choose from different views embedded in one video stream, with reduced data rate than simulcasting different views.

2.2 DRM System

In order to protect digital content from unauthorized access, the DRM (Digital Rights Management) system proposed uses device content packaging techniques that are applied to the digital items being protected. The packaging techniques used comprise content encryption and association of the encrypted content with a Digital Rights Object or license.

The system proposed aims to provide an end-to-end solution for content protection management for IP and P2P mobile networks, exploiting the full potential of the content protection and creator's rights maintenance. The aim is to offer innovative content protection via a personalized interoperable content protection solution, aiming to target all types of networks described in section 2.3. Thus, new business models for large scale content distribution will be facilitated side-by-side to a proper content protection and asset management mechanism.

In the following sections, the two technologies that are part of the DRM system proposed will be deeply explained.

The design of our solution is not only focused on developing a beyond state-of-the-art content protection technology, based on these two sides of the issue (specially targeting private content protection and superdistribution), but also to study the consumers' acceptability of the developed content protection mechanisms.

2.2.1 Content protection

The presented system covers the media protection mechanisms, using content protection based on ISMACryp [2] extensions for point-to-multipoint and point-to-point topologies, in the sense of real time encoding and decoding. This technology is embedded in the encoder and decoder of H.264 MVC/SVC.

2.2.2 License system

Another important point is the management of media assets, a really necessary improvement for the handling of user generated content and to be readily combined with content protection technologies.

The solution proposed aims to establish new media protection paradigms and solutions for P2P mobile networking using a lightweight asset management.

The license system contains all necessary information to enable the licenses creation and reproduction at the consumer. The

licenses are ODRL [3] documents, which specify permissions and constraints associated with a piece of DRM content. The system is designed in such way that DRM protected content cannot be used without its associated license; in other words, it may only be used according to the permissions and constraints specified within the license. The license accompanying protected digital items contains all necessary information, including the key to decrypt the content.

2.3 Multi-source/multi-network streaming & adaptation

The last technology pillar used is multi-source/multi-network streaming & adaptation. The proposed system places the user acting as content consumer, content mediator and content producer. Although the system is prepared for mesh P2P logical overlay technologies, it has been also prepared to broadcasting networks e.g. terrestrial (DVB-T), satellite (DVB-S/S2), cable (DVB-C), interactive/on demand bidirectional networks e.g. xDSL, WiMAX, mobile networks e.g. 3G/4G, GERAN, UTRAN, DVB-H.

Under building a service architecture upon the described variety of access networks, it is necessary to have as much information and adaptations at the lower layers as possible, along with the scalability functionality coming from the media codec.

2.4 Interoperability of the system

The RELs that cover a prominent role are ODRL (used in OMA) and MPEG-21 REL [4]. In the designed system, the content creator also creates the license in ODRL. In order to make the system compatible with others, the interoperability with other systems has been taken into account, so a conversion between ODRL licenses and MPEG-21 REL and OMA licenses has been considered.

Regarding OMA, the DRM proposed in the system follows the general concept scheme of the OMA DRM architecture. In fact, The OMA DRM Version 2.0 specification [5] extended the profile adopted in the OMA DRM Version 1.0 specification. The extensions included new elements, specific to the OMA community, and reuse of some of the standard ODRL data dictionary elements.

Regarding MPEG-21, both RELs, ODRL and MPEG-21 REL are based on XML. To transform an ODRL license into an MPEG-21 REL license, or vice versa, it is equivalent to transform a XML document into another XML document, where the information to represent is identical but with a different XML structure. To obtain this transformation, XSL (Extensible Stylesheet Language) is used, more specifically XSLT (XSL Transformation) as shown in Figure 1.

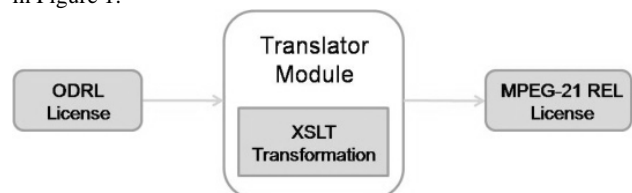


Figure 1. XSLT Transformation

3. ARCHITECTURE FOR SECURE AND ADAPTABLE CONTENT DELIVERY

The architecture can be distributed or semi-distributed [6]. Distributed P2P architecture clients do not establish connection with a server to download a license necessary for content presentation in a secure content delivery. Although licenses are delivered through the network encrypted, this network architecture entails serious security problems. This model is inefficient if we want to encrypt and have consumption control over a set of media content. Digital content can be copied and redistributed without any restriction, which is in many cases undesired. Therefore, a first requirement is to design and develop a content management system with data encryption.

The content encryption entails a complex management system. Several modules performing different functions are necessary to develop a secure system for ensuring content availability through the network.

Therefore, the system to be implemented has the following functions:

- Users' registration and support of an updated database, containing information related to the available contents and licenses.
- License generation, encryption and management.
- Identification of which licenses belong to which content
- Establish communications between the clients of the P2P network and the server.

Taking into account these requirements, the architecture chosen is a semi-distributed P2P based architecture: the core functions are located in the separated DRM server whereas the rest lie in the peer nodes.

The system proposed is a SVC/MVC content management and secure sharing system. The system is divided into server side and client side. The Server carries the DRM functions, by means of the following basic actions:

- a) Processing peers' registry.
- b) Generating and issuing ECM messages.
- c) Providing the EMM datagram, including the license, to the peer who has requested a piece of content.
- d) Managing databases with the information of the content and its licenses.

Compared to a centralized system, the functions of content storage and download services have been removed. But compared to a distributed rights system, we take the function of issuing licenses and publishing content information back from peers to the server side. The key management system is included in the server, so that it entails all the functionalities the client needs to manage its content.

On the other side, the Client, has the function of a normal peer, which can be resumed in the following:

- a) Encrypting content
- b) Generating keys for encrypting the content
- c) Creating, encrypting and sending licenses to the server
- d) Reading and interpreting licenses

- e) Providing contents to other peers

3.1 Solution implementation

In this section, we detailed all the elements implicated in the architecture we propose as a solution for a lightweight management of scalable and personalised media in mobile IPTV networks.

In order to provide security to the system we need to encrypt the content that will be sent to the P2P network. This functionality has been implemented using the ISMACryp standard. Moreover, to create a more secure system, the control word (CW) used to encrypt the content is encrypted and sent in an ECM (Entitlement Control Message). To achieve this, we have followed the DVB SimulCrypt specification [7]. Then we send the license by an EMM (Entitlement Management Message) as explained in [7].

Besides, we need to manage the content licenses to provide a user with the correct license for content presentation. Key management is also important and is considered in our solution.

Therefore, as it can be seen in Figure 2 the principal system modules located at the server are the ECM Generator (ECMG), the EMM Generator (EMMG), the key management system and the license management system. In next lines we explain deeply the function of each module.

On the one hand, the ECM generator creates an ECM message, which includes the Control Word (CW) that has been used to encrypt the content, following the ISMACryp standard, and some other parameters needed to establish connection between this particular module and the SCS module. On the other hand, the EMM messages are generated by the EMM generator module, also included in the server. An EMM contains the license which indicates the actions that a user can take upon a specified content and the necessary key to decrypt the encrypted CW of the ECM message.

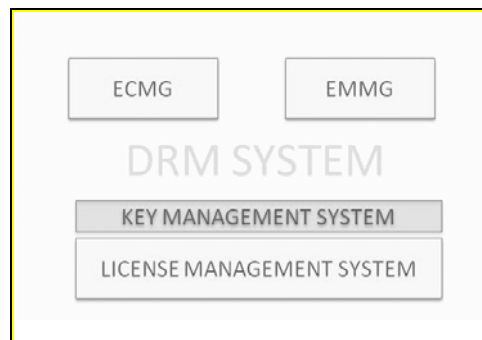


Figure 2. DRM system at the server side

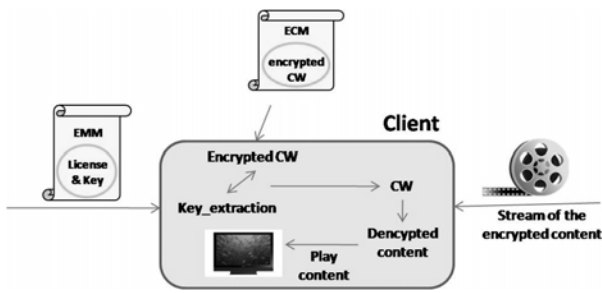


Figure 3. Interaction between ECM and EMM messages.

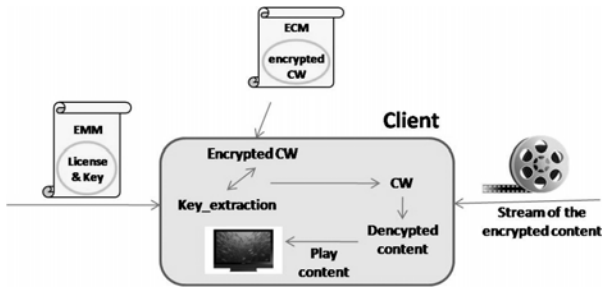


Figure 3, shows the ECM and EMM messages functions and the interaction between the information they carry inside, at the client side.

In order to control all the keys that get into the action, the system we propose includes a key management system. The key management involves the generation, selection, and distribution of the key data to be used in the algorithm for the encryption. In the proposed DRM system, two different set of keys are implicated. One of them is needed to encrypt the CW generated by the ISMACryp encryption module. This encryption is done in the ECMG module. The other set of keys is needed to encrypt the license. This is done in the license management system.

Finally, regarding the license management system, it is divided into a client side and a server side.

At the client side, the system proposed includes a license creator and interpreter module. Both modules are integrated in the terminal media player. The license creator creates licenses including the rights that the content creator wants to give his/her content. The license interpreter module included in the player reads the rights within the license and plays the content according with the rights.

At the server side, we have included a license management system to provide the correct license to the user who has requested and paid for it (in case he needs to pay). To help accelerate peer discovering and license downloading we use a data base which is stored and published in the server side.

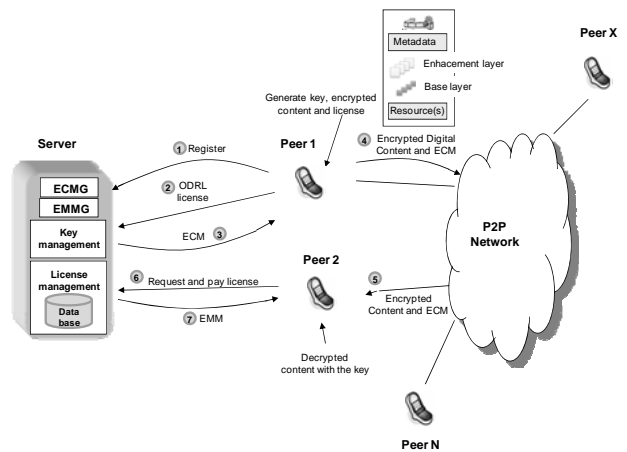


Figure 4. Content protection system over a mobile IPTV network

Figure 4 shows the system proposed for content protection in a mobile IPTV network.

In order to clarify all the functions of the modules previously explained and the interaction between them, a normal process of file sharing is shown in Figure 4:

- 1) Peer 1 has a content to share. First it registers to the server. The server creates at this moment a *user_ID*.
- 2) Peer 1 generates metadata (e.g. file name, file type, file length), and sets access rights to the content (e.g. the enhancement layer that the user can access). With this entire information peer 1 creates the license in XML and sends it to the server.
- 3) The server identifies the content and creates an ECM which is send to the user.
- 4) At this point, Peer 1 is able to encrypt the content. At the same time, the server stores the license in the database and associates it with the content. A license consists of right object, client's information (*user_ID*, *content_ID*) and encryption key. Right object is expressed in ODRL. The Server publishes content information on the Data Base to let other peers know that Peer 1 has issued a piece of content.
- 5) Peer 2 discovers from the data base that a piece of content is being distributed. It searches and obtains encrypted content in regular P2P manner.
- 6) At this moment, Peer 2 asks the server for a license.
- 7) The server sends an EMM message that contains the license to Peer 2. Peer 2 decrypts the content with the key included in the ECM that can be decrypted with the key of the EMM message, and executes the content as the right object authorizes it to.

To complete this system, we need to add some plug-ins into the media player of the mobile device. Firstly, an SVC codec plug-in to the client's media player is added. Thus, the content is available in several resolutions to satisfy different clients' needs. Also is added a plug-in to the media player to make it able to create and understand the licenses and execute the content as the right object authorizes to. Another fundamental action, included in the client environment, consists of a proxy that adds

ISMACryp encrypting and decrypting capabilities to the media player.

3.2 Use cases

According to the consumption permission given to the media content, we can distinguish several use cases that should be treated in our model. The encryption scheme combined with the proposed network architecture allows implementing a P2P network in which content can be introduced unencrypted if the author wants to distribute it freely, or encrypted if the author wants to take control over the users authorized to view that content. These use cases are described below:

1. Content that can be consumed by any user. A piece of content is introduced in the network without any restriction of consumption. Any user can acquire and consume it. There is no key for this kind of content because it is not necessary to decrypt it. The content carries the corresponding signaling information showing that it is unencrypted.
2. Encrypted content restricted to a set of users selected by the author. A user (creator) creates some content and gives permissions to consume it to a reduced group of users, for example, his friends. He encrypts it with a key and he introduces the content in the network. Now it can be distinguished two cases:
 - a) The creator allows his “friends” to distribute the content to other peers, so he/she sends them the key (e.g. by email, phone call, etc.) giving them the freedom to consume it whenever they desire.
 - b) The creator wants to have control over the content and avoid its consumption by another people. A user creates a piece of content and sets a series of restrictions for its consumption. There are different types of restrictions, such as:
 - The number of times that the content can be played: it depends on the kind of license the user owns. For example, the more expensive it is, the more times it can be played.
 - The layer to which a user has access to: the content protection mechanism can be applied to H.264 MVC/SVC encoder and decoder. The license system implemented provides the consumer with the chance of selecting the number of views and the number of layers the consumer wants to display, depending on the terminal capabilities or the consumer preferences. The selection of the consumer will be reflected in the license.

An example of the most critical use case (number 2) could be the following: a user has a content to share and creates two licenses. One license gives the consumer rights to see one view of the content and the other license gives the consumer rights to see two

views of the same content. The consumer buys the license that contains the rights to see two views and this parameter is included in the license, together with the key to decrypt the content and other rights such as the number of times the consumer can display the content, etc.

4. CONCLUSIONS

We have designed a solution for content protection and management in P2P mobile environments using personalized and adaptable video environments (SVC/MVC).

There are several technologies needed to create a system with all these functionalities. These technologies have been described in section 2 and proof the complexity of the whole system. It is important to mention the different kind of environments where the system described can be implemented and used.

A general architecture has been described, including the licenses managers, encryption mechanisms, key management elements, mediators, etc., which is fully compatible and adapted to a SVC/MVC content delivery network. In addition, the content management system has been defined to be interoperable with as much standards as possible, ensuring a real seamless content delivery across heterogeneous networks and terminals.

5. ACKNOWLEDGMENTS

This publication is based on work performed in the framework of the project SEA IST-214063, which is partially funded by the European Community. The authors would like to acknowledge the contributions of colleagues from: STM, Synelaxis, Thomson GV, Philips, Vodafone, Nomor, Fraunhofer HHI, Politecnico di Torino, Universidad Politécnica de Madrid and University of California, Los Angeles.

6. REFERENCES

- [1] SEAmless content delivery project: www.ist-sea.eu
- [2] Internet Streaming Media Alliance Encryption and Authentication Version 1.1. <http://www.isma.tv>
- [3] Open Digital Rights Language (ODRL) Version: 0.9 Date: 2001-06-29 URI: <http://odrl.net/0.9/ODRL-09.pdf>
- [4] Delgado, J., Prados, J., Rodríguez, E. “A new approach to interoperability between ODRL and MPEG-21REL”.
- [5] OMA (2004). Open Mobile Alliance DRM Specifications, Version 2.0 Candidate Enabler, July 2004 http://www.openmobilealliance.org/release_program/drm_v2_0.html
- [6] Jae -Youn, S., Jeong -Yeon, J., Ki -Song Y. DRM Enabled P2P Architecture. UST, Computer & Software Engineering Dept. ETRI, Digital Contents Distribution Research Team.
- [7] Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt, ETSI TS 103 197 V1.4.1, September 2004.