

SVC/MVC Content Protection over P2P Delivery Networks

Lara García (1), Laura Arnaiz (1), Federico Álvarez (1), Theodore Zahariadis (2)
 (1) Universidad Politécnica de Madrid (GATV), (2) Synelixis

Abstract—In the present paper a novel system and its architecture is presented. The aim of this system is to enable personalized view, scalable, seamless and trusted multimedia content delivery, while protecting content from unauthorized access. Moreover, the system aims to keep bandwidth requirements low and increase the Perceived Quality of Service (PQoS). This content delivery is done through multiple kinds of networks. Special attention to content protection and license management and the possibilities of the system to provide adaptable content to the user thanks to the scalable and multi view video coding is made.

I. INTRODUCTION

Widespread and affordable broadband access opens up opportunities for delivery of new streaming services. It is expected a change in the way people use the network, in a 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).

In this way, it is important to offer the users adaptable and personalized contents through multiple kinds of networks and terminals. Two of the main coding technologies to offer both features are 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 P2P network, content should be properly protected to be able to be decoded uniquely by the targeted user. Adaptable and personalized contents over P2P networks need special tailored content protection mechanisms which we will further describe in the paper.

In next section II, we describe the key technologies used in the proposed system. Later, in section III, we present the system's architecture, specially the license management procedure. And last, in section IV, the possible interoperability between this solution and other based on different RELs (Rights Expression Languages) will be explained.

II. KEY TECHNOLOGIES

The proposed architecture provides a novel functionality to the system through the combination of new technologies and different kinds of networks, including content protection [1].

One of these technologies is the Multi-layered/Multi-viewed content coding. For the proposed architecture it is considered H.264 SVC and H.264 MVC as the major foreseen content delivery technologies over heterogeneous network.

SVC offers layered temporal/spatial/quality content scalability, whereas MVC introduces a truly personalized video delivery experience by allowing the user to select among the different views embedded in a single video stream.

Another important technology is the content protection. In this way new business models for large scale content distribution will be facilitated side-by-side to a proper content protection and asset management mechanism. The aim is to offer innovative content protection via a personalized interoperable content protection solution, aiming to target all types of networks described in this section.

We cover the media protection mechanisms using both necessary sides of the problem: on the one hand, the technologies to be embedded in the encoder and decoder of H.264 MVC/SVC, using content protection mechanisms based on ISMACryp[2] extensions for point-to-multipoint and point-to-point topologies, in the sense of real time encoding and decoding, and on the other hand the solutions for content protection and rights management solutions for new media in P2P networks, based on the adaptation of standardized solutions such as MPEG-21.

The design of our solution is not only to develop 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 content protection mechanisms developed.

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 the content protection technologies presented.

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 with the media codec.

III. ARCHITECTURE FOR SECURE AND ADAPTABLE CONTENT DELIVERY

In this section, we propose a SVC/MVC content management and secure sharing system [3]. By now this

system has been implemented in our laboratory and will have practical applications in the near future. Our system is divided into server side and client side [4]. To avoid building up the workload, we propose a light-weight system, with four basic functions: (a) processing peers' registry (b) generating and issuing the key to the user that needs to encrypt the content; (c) publishing content information; (d) providing with the license to the peer who wants to have access to the whole content.

The first and second functions do not increase much payload onto servers as content storage and download services do. Therefore, compared to centralized system, we eliminate the function of content storage and download services, but compared to distributed system we take rights of issuing licenses and publishing content information back to the server side from peers. We include the key management system in the server, so that it has all the functionalities the client needs to manage its content.

Client, in the proposed system, is a normal peer with a list of functions: (a) encrypting content; (b) creating and sending content license to server; (c) providing contents to other peers.

For the implementation we chose VLC media player (www.videolan.org) a highly portable multimedia player for various audio and video formats as well as various streaming protocols. To complete our system, we need to add some plug-ins into the VLC media player. Firstly, we added a plug-in in order to add SVC capabilities to the client's VLC media player. Thus, the content is available in several resolutions to satisfy different clients' needs. Other plug-in included in the client environment adds encryption capabilities to the VLC following ISMACryp. Finally, we also needed to add a plug-in to the VLC to make it able to understand the licenses and execute the content as the right object authorizes to. The increase of the processing power due to the use of a content management system is only given by the plug-ins as the majority of the data processing is done in the intermediate servers. The system is perfectly capable of working under the computational capabilities of both stationary and mobile receivers.

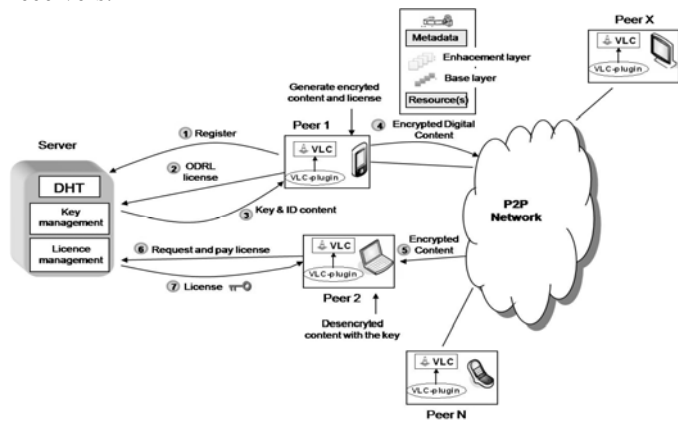


Fig. 1. Content protection and key management system overview

To help accelerate peer discovering and content downloading we use DHT (Distributed Hash Table) which is

stored and published in the server side.

Fig. 1 shows the system that we proposed for content protection and key management system. A normal process of file sharing is: (1) Peer 1 has a content to share, at first it registers to server; (2) Peer 1 generates metadata (e.g. file name, file type, file length, etc.), and sets access rights to the content (e.g. the enhancement layer that the user can access to). Peer 1 sends this information to the server in XML. (3) Server generates the key to encrypt the content and identifies the content by assigning it an identifier (*content_ID*). Afterwards, server sends both, key and identifier, to Peer 1. At this point, Peer 1 is able to encrypt the content (4). At the same time, the server creates the License according to metadata, access rights and Peer 1's private information and stores it in the database. A license consists of right object, client's information (*user_ID*, *content_ID*) and encryption key. Right object is expressed in ODRL. Server publishes content information on DHT to let other peers know that Peer 1 has issued a piece of content. (5) Peer 2 discovers from DHT that a piece of content is being distributed. It searches and obtains encrypted content in regular P2P manner. (6) Peer 2 asks server for a license. (7) Peer 2 decrypts content with the key included in the license, and executes the content as the right object authorizes it to.

IV. INTEROPERABILITY OF THE SYSTEM

The RELs that cover a prominent role are ODRL (used in OMA) and MPEG-21 REL [5]. In the described system an ODRL license is generated by the user. Nevertheless the interoperability with other systems has been taking into account, so a conversion between ODRL licenses and MPEG-21 REL licenses has been considered.

Both RELs 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 to 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 Fig. 2.

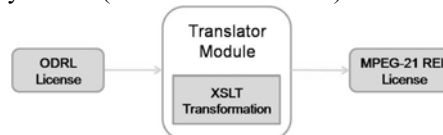


Fig. 2. XSLT Transformation

V. REFERENCES

- [1] SEAMless content delivery project: www.ist-sea.eu
- [2] Internet Streaming Media Alliance Encryption and Authentication Version 1.1: www.isma.tv.
- [3] T. Zahariadis, O. Negru, F. Álvarez. "Scalable content delivery over P2P convergent networks" 12th IEEE International Symposium on Consumer Electronics, ISCE 2008
- [4] Yang Liu, Chun Yuan, and Yu-Zhuo Zhong. "Implementing Digital Right Management in P2P Content Sharing System"
- [5] J. Delgado, J. Prados, E. Rodríguez. "A new approach to interoperability between ODRL and MPEG-21REL"