Network Centric Mobile Digital Rights Management for Multimedia Content

Sridhar, G., Sridhar, V., Chu, C-C.*, and Gadh, R*

Applied Research Group, Satyam Computer Services Ltd.,
* UCLA, Los Angeles, USA
{sridhar_gangadharpalli, sridhar}@satyam.com, {peterchu, gadh}@ucla.edu

Extended Abstract

Digital Rights Management (DRM) is a value-added service being strongly considered by Network Service Providers (NSP) and Content Service Providers (CSP). Tracking the distribution of multimedia to the mobile clients they service poses several DRM challenges. Digital rights needs to be enforced seamlessly yet retaining flexibility and ease of use. Effective mobile DRM solutions support not one, but multiple business models, preventing unauthorized copying and distribution. In this paper, we propose a network-centric DRM solution designed to be transparent and non-intrusive. The two primary components of this architecture are DRM monitoring for post verification and DRM enforcement of select digital rights. The first, DRM monitoring, is achieved by recording DRM transaction messages sent through a secured DRM channel. The second component, DRM enforcement, is accomplished by embedding digital rights enforcement codes along with a key into the encrypted content. With the two-component network centric approach, NSP could track multimedia delivery and usage condition and effectively enforce DRM to prevent piracy.

Monitoring of transaction records of multimedia contents allows CSP and NSP keep track of content ownership and usage status. In general, these monitoring operations and activities are required to 1) protect privacy – content ownership is kept confidential; and 2) to be non-intrusive – transaction records are logged without user intervention. In the current approach, non-intrusiveness is achieved by using a private DRM channel established between base station and terminal device to transmit DRM transaction records. Privacy is protected by attaching a globally unique ID to each piece of content delivered to a subscriber. The DRM channel is a signaling and control channel that is established on power-on between a mobile terminal and a base station. This channel is used for communicating messages related to content delivery with least overhead.

For DRM enforcement, we propose an approach for enforcing two distinct kinds of rights, namely, single-view rights and multi-view rights. Single-view rights, as the name indicates, permit the user to view the content only once and Multi-view rights allow multiple viewings by permitting the user to locally store the content. Our approach is to addresses the challenge of enforcing these rights even under hardship circumstances.

During broadcasting, it is essential to protect the content from unauthorized content manipulation. In our approach, the CSP and NSP jointly enforce the DRM with support from device functionality. This approach relies on embedding both the rights enforcement code and a key into the encrypted contents at the NSP, and obtaining the decryption key by executing the rights enforcement code. In order to avoid accessibility to plain content, Just-in-time Decryption (JID) is used. With JID, decrypted information is available as briefly as possible and only in very small chunks at a time. In this approach, byte-by-byte decryption is performed such that plain contents in display registers are available for too short a time period for manipulation to occur. The approach for DRM enforcement makes use of the support extended by hardware and OS of the mobile device. The FPGA-based Just-in-time Decryption enables real-time control on digital rights while DRM enabled OS monitors digital contents whenever the device power is on.

The proposed approach provides a solution for enforcing digital rights and at the same time monitor the content usage with respect to the granted rights. The main aspect of this approach is to exploit the support from the OS to achieve effective monitoring of the content usage.

Presented at CCNC 2005 Workshop on Digital Rights Management Impact on Consumer Communications - 6 January 2005,Las Vegas, Nevada, USA