Mobile DRM for Multimedia Content Commerce in P2P Networks

Chu, C-C, Su, X., Prabhu, B.S., Gadh, R., Kurup, S., Sridhar, G., Sridhar, V.
University of California – Los Angeles,USA and Satyam Computer Services, India

Abstract

In this paper, the requirements for multimedia content sharing among Peer-to-Peer (P2P) networks are investigated and novel business models along with Digital Rights Management (DRM) solutions are proposed. In the current approach, to provide least intrusion and interference for end content consumers, content providers are not involved in the communications or peer transactions of P2P networks after the multimedia content are sold to the peer users. Peer users may legally trade or exchange their content within the P2P network via the proposed Ticket and Credit based Multimedia Commerce (T&C Commerce) system. The aim of this DRM research is to set new business models for multimedia content owners and retailers to benefit from the massive power of content distribution of P2P networks with least intrusion and interference to end consumer's privacy and anonymity.

1. Introduction

Recent advances in wireless communications, mobile devices, streaming technologies and compression techniques have made possible the broad distribution of multimedia content such as digital music, image, video and games over the Internet. Mobile devices are rapidly becoming the means to extend the range of communication and entertainment channels [1]. Multimedia content are sold not only in physical media format, such as CD, DVD, but also in digital media format over wired and wireless networks. Without proper management and authentication procedures, multimedia content may be illegally altered, copied and distributed among unauthorized terminals. These copyright infringements directly affect multimedia content revenue, posing a major financial threat to the media production industry [2].

Digital Rights Management (DRM) is a technology that allows content owners or content retailers to securely sell and distribute multimedia content in digital format over computer networks. The primary requirement of DRM systems is to allow individuals to consume the digital content according to the digital rights purchased from content retailers. Cryptographic and watermarking technologies are commonly used techniques to incorporate digital rights, media identification, and tracking information in the content [3, 4]. The encrypted multimedia content is distributed to the client device where it is decrypted and consumed using the license or key purchased from content retailer. In general, multimedia content retailers are required to host DRM servers to authenticate clients, issue encrypted content, billing the clients, and manage clients' content rights/licenses. In this scenario, strong network backbones for supporting simultaneous large content streaming is required and this poses great scalability challenges and causes additional investments for the content retailers. In addition, content retailers need to actively monitor and authenticate end user transactions to prevent illegal content distribution and malicious actions from clients. Content retailers need to take persistent security precautions to protect their digital assets.

Another concern in the DRM systems is the privacy and anonymity issues of content consumers [5]. Since DRM systems track user transactions, purchases, and access history, end consumers' detail activities are recorded at content retailer's database and thus raise divergences regarding multimedia content protection versus privacy protection.

P2P networks are self-organizing distributed systems where participating nodes provide and receive services from each other in a shared collaborative environment without distinguished roles as pure clients or pure servers. P2P file sharing systems such as Gnutella, Freenet, KaZaA, and BitTorrent [6, 7] gives peer users the freedom to communicate and collaborate with each other one-on-one without a server in the middle. With the P2P network communication, multimedia content are efficiently and rapidly distributed among end users. However, lawsuits has been filed against these P2P file sharing systems as the content owners have sustained revenue atrophy from privacy and copyright abuses.

In this paper, an innovative business model is proposed for multimedia content distribution among wired and wireless network. The corresponding DRM approaches utilize client side application and tamper resist hardware to enforce digital rights. The proposed

In the proceeding of IEEE CCNC 2006 Workshop on Digital Rights Management Impact on Consumer Communications – 8-10 January 2006, Las Vegas, Nevada, USA.

business model and DRM system are based on the requirements of a P2P network which consists of fixed and mobile terminals with decentralized P2P content distribution. Multimedia content are efficiently distributed and legally consumed among peers without monitoring and interference from content retailer. The aim of this DRM research is to set new business models for multimedia content owners and retailers to benefit from the massive power of content distribution of P2P networks with least intrusion and interference to end consumer's privacy and anonymity.

2. Previous DRM and P2P Approaches

In multimedia content distribution industry, multiple parties are involved along the value chain of content creation, content management, content delivery, and content usage. Proper revenue distribution along this value chain calls for a comprehensive approach towards DRM and content download standards. Several organizations in this value chain have formed the "Open Mobile Alliance" (OMA) [8] which has contributed significantly to the evolving, DRM-supporting mobile architecture standards. These standards provide a global framework for content messaging, delivery, and intellectual property management. OMA uses a rights expression language based on Open Digital Rights Language (ODRL) developed by IPR systems [9]. This allows OMA to support a profile that includes 1) permissions: play, display, execute; and 2) constraints: count, data range, time period.

There are existing commercial DRM systems which use their own proprietary approaches and specific client side applications or plug-ins. Examples of these systems include Microsoft Windows Media Rights Manager [10], RealNetworks Helix DRM [11], IBM EMMS[12], … etc. Development of DRM systems is still at its early stage. There has not been a comprehensive DRM system yet that is widely used in the multimedia content distribution market.

P2P networks have recently gained much attention due to its advantageous features of decentralized administration, load balancing, fault tolerance, and recovery [13]. Using hopping technologies, peers that are out of range of the peers they wish to communicate with can hop through other peers to reach their destination through either wired or wireless networks. This greatly extends overall communication range and provides countless conveniences for mobile users [14]. With these valuable features, P2P networks serve as an ideal communication infrastructure for massive multimedia content distribution over mobile and wired networks.

Existing approaches for DRM over P2P networks usually involve a centralized server being designated as an authority for the registered peers and as a facilitator in network operations such as peer authentication and transaction monitoring [15, 16]. In the multimedia content distribution scenario, this server is usually hosted and maintained by the content providers. This results in peer user's anonymity interference and content provider's efforts in server maintenance.

In the current research, we studied the requirements of P2P multimedia content sharing networks and proposed business models and DRM solutions that are based on peer side hardware authentication and transaction monitoring. In this approach, content provides are not involved in the communications of P2P networks after the multimedia content are sold to the peer users. Peer users may legally trade or exchange their content within the P2P network via the client side P2P application. The details of this business model and its DRM approaches are discussed in the following sections.

3. Multimedia Content Commerce

Multimedia Content Commerce refers to the buying and selling of digital media over networked terminals. Within P2P networks, the identifications of peer terminals are kept anonymous and no centralized server is needed for peer monitoring and authentication. Multimedia content are freely distributed and legally consumed to maximize the benefits of both content provider and end consumers. Based on these guidelines, a multimedia content commerce business model: Ticket and Credit based Multimedia Commerce (T&C Commerce) is proposed

3. 1. T&C Commerce

The following rules are applied to this business model:

1. Multimedia content are distributed in digital encrypted format. The same encrypted content may be viewed by specific tickets (digital keys).
2. A ticket is consumed and can only be used once for viewing a particular multimedia content during a time period after its initial usage.
3. Tickets are purchased from content provider in bulk amount. Along with the purchased tickets, credits are awarded to the peer user based on the amount of tickets purchased.

4. Credits may be used to purchase other content tickets from peer users. Ticket seller receives credits from buyer when the ticket is delivered. The default price for a ticket is one credit.
5. Peer users may set the prices (in credits) of the tickets they own based on the popularity of the corresponding content. There is a minimum limit on the price of a ticket.

Figure 1 illustrates an example of T&C Commerce on a P2P network.

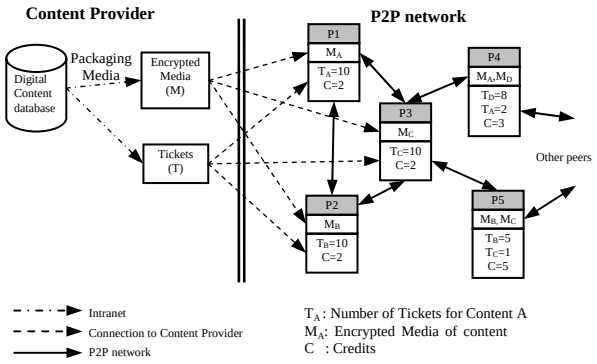

Figure 1. An example of T&C Commerce

As shown in Figure 1, content provider packages original multimedia content into encrypted multimedia (M) and generates tickets (T) within the intranet. Dot-dashed lines represent the dataflow within the content provider's intranet. In the P2P network, a peer user P1 purchases 10 tickets of content A (T_A=10), receives 2 credits for this purchase (20% of the tickets purchased) and receives the encrypted multimedia content A (M_A). Dashed lines represent the dataflow when peer users purchase from content provider. In a similar manner, P2 and P3 purchased tickets for content B and content C, etc. Within the P2P network, peers users are interconnected with each other as shown in solid lines in Figure 1 and may use the tickets they purchased to view the content or use the credits to purchase tickets of other content from other peer users.

After purchasing from the content provider, peer users may perform the following actions or transactions with other peers without connecting to the content provider for authentication: 1) use the purchased tickets to view the content, 2) advertise the content and tickets he/she owns (set the price in credits) on the P2P network, 3) search the availability of multimedia content he/she wants, 4) purchase tickets from other peers with credits, and 5) purchase more multimedia content from the content provider. Table 1 shows some sample actions and transactions in the P2P network. In Table 1, the first column lists the actions/transactions in step sequence and the other columns list the remaining multimedia content, tickets and credits balances of each individual peer users after that step. The dollar sign "$" and the amount adjacent to tickets indicate the price of that ticket in credits. Notice that in 3-rd step, P2 raises T_B price to $2 credit due to its popular demands. After certain actions and transactions between peers, in the n-th step, P3 still cannot sell any T_C and he has used up all his credits. In order to earn credit for purchasing other multimedia content, P3 reduces T_C's price to $0.5 credit to attract other peers to buy T_C from her/him.

Table 1. Sample actions and transactions

Steps of actions / transactions	P1	P2	P3	…
1. initial status	M_A T_A=10, $1 C=2	M_B T_B=10, $1 C=2	M_C T_C=10, $1 C=2	…
2. P1, P2 and P3 use one of their own tickets to view the content they own. P1 purchase 2 T_B from P2	MA, MB TA=9, $1 TB=2, $1 C=0	M_B TB=7, $1 C=4	M_C T_C=9, $1 C=2	…
3. P1 sold 3 T_A to other peers and use 1 T_B, P2 raise T_B price to $2, and P3 purchase 1 T_B from P2 and use the ticket	M_A, M_B T_A=6, $1 T_B=1, $2 C=3	M_B T_B=6, $2 C=6	M_C, M_B T_C=9, $1 C=0	…
…	…	…	…	…
n. P3 reduce T_C to $0.5 and sell 3 ticket to P2	M_A, M_E, M_B T_A=2, $1 T_E=3, $1 C=1	M_B, M_D, M_A T_B=1, $2 T_D=2, $1 C=4	M_C, M_B T_C=9, $0.5 C=0	…
…	…	…	…	…

3.2. Considerations

In this business model, members of the P2P network actively participate in the distribution of multimedia content as they need to sell their unused tickets to earn credits for purchasing other content tickets. The fact that P2P members are allowed to set their own price (in credits) for their available tickets make this P2P network a multimedia content commerce. Members may dynamically adjust their prices for the tickets they own according to the popularity and availability of the content. For example, if P1 purchases an unpopular content he/she may reduce his price to attract buyer. On the other hand, P1 may own a very popular content and it may also not be available anywhere else in the P2P network he/she is in, then P1 may increase the price to acquire more credits from selling this content.

Content provider should not sell only credits to the P2P members as it would quickly lead to a situation where peer users have only credits but no tickets left in the P2P network. The only two ways to acquire credits

are 1) through purchase of bulk content tickets and get credits, and 2) sell the ticket he/she owns and earn credits. The primary purpose of credits awarded during the initial bulk ticket purchasing is to allow a peer user the ability to purchase other tickets when he/she first joins the P2P network. Another extreme situation to avoid is when all peer users are left with only tickets without credits in the P2P network. In this case, peer users may choose to consume these tickets themselves; or purchase more tickets from content providers and earn credits. Since credits are transferred among peer users and will always exist within the P2P network without being consumed, the content providers are required to re-collect them as the P2P network grows. Content providers may offer extra tickets for the earned or unused credits when the peer users come back and purchase bulk content tickets again. Peer users should not trade in all of his credits and must maintain a certain amounts of credits so that they retain the ability to purchase content from other peers.

3.3. Revenue Integration

In the current T&C Commerce business model, multimedia content are sold by viewing times i.e. consumers purchase tickets to view a multimedia content and can only view the content for a limited time and during a limited time period. Content providers' revenue come from the integration of content viewing times instead of copies of content sold. A typical multimedia content, such as movie, may go through different stages after its initial release. Figure 2 shows a plot of this revenue analysis.

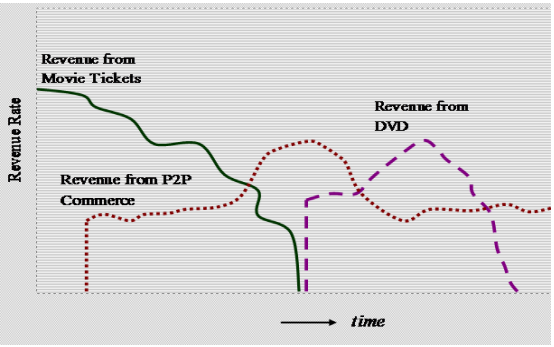

Figure 2. Revenue Analysis

In Figure 2, in the initial stage of release of a multimedia content, revenue is largely obtained from sale of movie tickets from theaters. While the theaters continue to add to the revenue generated, the P2P commerce for the content also starts shortly, but on a lower scale, since initially most people would prefer to watch the movie in the theaters. The rationale behind allowing P2P commerce to start early is due to DRM enforcement which reduces the piracy concerns in P2P Commerce. Finally when theaters do not play the movie any more, the P2P commerce tends to catch up and gains high revenues for the content, but starts dropping as the sales for DVDs start and catches up. However the revenue generation period for DVDs is also short lived and drops down relatively fast. With P2P commerce being supported by DRM enforcement and driven by multiple viewings of the content, the content providers are able to gain revenues from it over a much longer period of time. Revenue considerations in the proposed business model are as follows:

$$R = \int_{t=0}^{t=\infty} P(t)F(N,U,D,t)dt \qquad \text{where,}$$

R: total revenue of one multimedia content
N: number of P2P networks for a content provider
U: number of peer users
D: number of devices a peer user have
P: revenue gain in dollars when the content is consumed at any given time
F: total number of viewings at any given time, function of *N*, *U*, *D* and *t*
t: time, *t=0* is the time of initial release of the multimedia content

3.4. DRM Implementation

In the current approach, DRM is enforced by client side application and hardware based authorization. The client side application is installed on the client terminal and is responsible for P2P network communication, processing T&C commerce transactions, and managing multimedia content tickets. Sensitive data such as user credit balance, multimedia tickets (decryption keys), and selling prices of tickets are encrypted. The encrypted data is stored in a protected area of a tamper-free hardware that is only accessible to authorized client side application. Smart Cards and Security Digital Cards are examples of such tamper free hardware devices [17, 18].

When peer users initially purchase bulk tickets from content provider, they are issued client application and the tamper free hardware. A secret key is issued and embedded on the client application and hardware, encrypted and is known only to the client application and its corresponding hardware. Only with this key can the protected data be accessed on the hardware. In addition to handling P2P network communication and processing secure T&C commerce transaction, the client applications are required to have the following functionalities:

Content discovery: allows the peer user search the content title within the P2P network and provide information on viewing requirement.

Content wish list: allows the peer user to create a list of desired content list and notify the user when the content is available in the P2P network.

Trailer super-distribution: allows peer users to freely download, distribute and view trailer.

A sample client application screen shot that indicating these functions is shown in Figure 3.

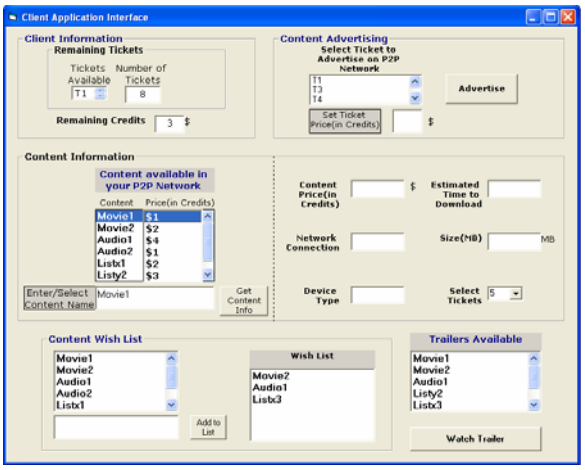

Figure 3. A sample client application screen shot

4. Summary

In this paper, an innovative business model for multimedia content distribution among wired and wireless P2P network is proposed – T&C Commerce. The corresponding DRM approaches are presented, utilizing client side application and tamper resistant hardware to enforce digital rights. Multimedia content are efficiently distributed and legally consumed among peers without monitoring and interfering from content retailer through the use of tamper resistant Smart Cards or Secure Digital Cards which store and update sensitive information such as remaining number of tickets, available credits, content expiration date, etc. In this approach, there is no central server management to track user credit or ticket and thus peer users' anonymity is preserved. The aim of this DRM research is to set new business models for content owners to benefit from the massive power of content distribution of P2P networks with least intrusion and interference to end consumer's privacy and anonymity.

5. Acknowledgment

The authors would like to acknowledge sponsorship from Intel Corp. and Wireless INternet for Mobile Enterprise Consortium (WINMEC) at UCLA in supporting this work.

6. References

[1] Lund, T., "DRM 101 – Digital rights management in a wireless world", May 2004 issue, Wireless Business and Technologies, Sys-Con Media Publication.

[2] Simon Byers, Lorrie Cranor, Dave Korman, Patrick McDaniel, Eric Cronin, "Analysis of Security Vulnerabilities in the Movie Production and Distribution Process", ACM Workshop DRM'03, October 27, 2003, Washington, DC, USA.

[3] Hartung, F. and Ramme, F., "Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications," IEEE Communications Magazine, vol. 38, issue 11, Nov. 2000, pp. 78-84.

[4] Mobasseri, B.G., "Ordered Bitplane Watermarking of Digital Video by Direct Sequence Spread Spectrum," International Workshop on Multimedia Database Management Systems, Aug. 1998

[5] Feigenbaum, J., Freedman, M., Sander, T., Shostack, A., "Privacy Engineering for Digital Rights Management Systems", The ACM Workshop on Security and Privacy in Digital Rights Management 2001.

[6] About.com, "Digital music: file sharing programs", http://mp3.about.com/od/filesharingprograms/

[7] Pasick, A., "File-Sharing Network Thrives Beneath the Radar", article on Reuters website, November 6, 2004, http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=6734497&section=news

[8] OMA-DRM-ARCH-V2_0-20030901-D, DRM Architecture , Draft Version 2.0 – 01, Open Mobile Alliance, Sept. 2003.

[9] IPR Systems, "Open Digital Rights Language (ODRL) – IPR Systems", http://www.iprsystems.com/

[10] Microsoft, "Windows Media DRM 10", http://www.microsoft.com/windows/windowsmedia/drm.aspx

[11] RealNetworks, "Helix DRM 10 from Real", http://www.realnetworks.com/products/drm/index.html

[12] IBM EMMS, "Electronic Media Management System", http://www.ibm.com/software/data/emms/

[13] OpenP2P.com, http://www.openp2p.com/

[14 Milojicic, D., Kalogeraki, V., et al, "Peer-to-Peer Computing", Technical Report HPL-2002-57, HP Lab, March 8, 2002.

[15] Iwata, T.; Abe, T.; Ueda, K.; Sunaga, H., "A DRM system suitable for P2P content delivery and the study on its implementation", Proceeding of the 9th Asia-Pacific Conference on Communications (APCC 2003), September 21-24, 2003, Vol. 2, pp. 806-811.

[16] Reti, T., Sarvas, R., "DiMaS: distributing multimedia on peer-to-peer file sharing networks", Proceedings of the 12th annual ACM international conference on Multimedia, October 10-16, 2004, pp166-167.

[17] SmartCard Alliance, http://www.smartcardalliance.org/

[18] SD Association, http://www.sdcard.org/