A Trust Model based DRM technology on Distributed P2P and IPv6 Networks

Aina Sui, Yongbin Wang, Rui Lu, Cheng Yang Communication University of China

Abstract—**P2P content sharing is often blamed for copyright infringement, making the establishment of DRM technologies an urgent need. A novel PCADRM (P2P-based Content Access Digital Rights Management) system is proposed. It is based on a trust model that focuses on content security, rights management and access control. Encryption, digital watermarking, and packaging technologies are adopted to protect the confidentiality and integrity of contents, and support copyrights verifying and piracy tracing. The structure of rights management integrates the distributed and centralized modes, which not only reduces the burdens of networks and rights server, but also provides controllability. The contents downloaded on the P2P and IPv6 networks can be played only with rights control. To realize access control, the password and identity authentication are used. The PCADRM system is implemented to prove that it can provide a more robust Intellectual Property protection solution for P2P content delivery.**

I. Introduction

With widespread use of the Internet and improvements in high value and interactive radio and television, many digital media resources can be distributed instantaneously across the Internet to end users. However, without protection and management of rights, digital contents can be easily copied, altered, and distributed, which could cause revenue loss to media companies. To protect commercial digital Intellectual Property (IP) and avoid digital piracy, we need DRM (Digital Rights Management) system that prevents unauthorized access to digital contents. There are a number of DRM solutions on the market, such as, Microsoft's Windows Media Rights Manager (WMRM), IBM's Electronic Media Management System (EMMS), InterTrust's Rights|System, and RealNetworks's RealSystems Media Commerce Suite (RMCS)[1][3].

Unfortunately, P2P networks have grown rapidly in information sharing to havens for trafficking in unauthorized copies of Intellectual Property. P2P file sharing systems, such as Napster, Gnutella and KaZaA, allow contents to be shared between distributed peers with many desirable features: adaptation, self-organization, load-balance, fault-tolerance, low cost, high availability, scalability, and a large pool of resources. Most P2P networks do not have any digital rights management or access control. P2P networks are often blamed for illegally sharing copyrighted materials[2][3].

There are many DRM technologies, however most of them are applicable only to conventional client/server based content delivery. A few DRM products are applicable to P2P content delivery. Guofei Gu etc. propose a PLI (Public License Infrastructure)-based DRM system to provide content protection and digital rights management for users of Peer-to-Peer (P2P) networks. The system is the first distributed DRM license service system, which is especially useful for small content providers such as peers in a P2P network[2]. Other researchers also have pay attention to integrating DRM with P2P networks, such as Tetsuya Iwata etc. of NTT Corporation studying on a DRM system suitable for P2P content delivery[4], Bill Rosenblatt of GiantSteps Media Technology Strategies studying on integrating DRM with P2P networks[5], Paul Judge and Mostafa Ammar of Georgia Institute of Technology studying on the benefits and challenges of providing content protection in Peer-to-Peer Systems[6].

This paper's research is from the project "The Middle Ware System for Media Resources Storing and Obtaining based on IPv6 and P2P Network" for National Development and Reform Commission. In this paper, a novel PCADRM (P2P-based Content Access Digital Rights Management) system is proposed for content protection in P2P and IPv6 networks that will allow content providers to safely delivery their film and television media materials.

The paper is organized as follows: Section 2 introduces the PCADRM system architecture. Section 3 discusses the method and format of content packaging, which includes encryption and digital watermarking. Section 4 introduces the content delivery based on P2P. Then we present Right Agent (RA) that is the core of the system in section 5. Section 6 addresses the secure media player supporting DRM. And we conclude the paper in section 7.

II. The Architecture of PCADRM System

The requirement of DRM is from users and commercial application, mainly focusing on the content security, rights

Manuscript received December 6, 2006. This work was supported in part by the National Development and Reform Commission of China under CNGI-04-12-2A.

Aina Sui, Computer & Software School, Communication University of China, Beijing, China, 100024(phone: 86-10-65779546; e-mail: aina@cuc.edu.cn).

Yongbin Wang, Computer & Software School, Communication University of China, Beijing, China, 100024(e-mail : ybwang@cuc.edu.cn.).

Rui Lu, Computer & Software School, Communication University of China, Beijing, China, 100024(e-mail : lurui@cuc.edu.cn).

Cheng Yang, Information Engineering School, Communication University of China, Beijing, China, 100024(e-mail : yangcheng@cuc.edu.cn).

1-4244-0708-7/07/$20.00 ©2007 IEEE

control and copyright protection. In order to create a secure environment to protect the copyright for the programming, delivery and consuming of film and television media, the PCADRM system proposed in this paper should be secure, controllable, scalable, and support behavior monitor and post-tracing.

A. The Framework and Modules of PCADRM System

In PCADRM system, the contents with copyright desire will be packaged firstly. Then the content packaged may be delivered to peer-user through IPv6 networks. Before the content is played, the relevant right of content must be purchased. The figure 1 addresses the framework of PCADRM system.

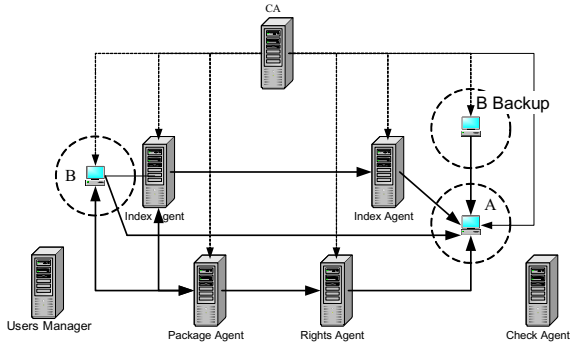

Fig. 1. the Framework of PCADRM System

The system process presented in figure 1 is as follows:

i. CA (Certificate Authority) presides over distributing identity certificates to the nodes in IPv6 networks.

ii. The node B calls the API of PA (Package Agent) to package the contents, and then informs Index Agent to create the indexes for contents.

iii. The node A can find a certain content position at B and B backup through Index Agent, and can download it from B and B backup.

iv. A can browse the usable rights and select to purchase one or more rights from RA (Rights Agent).

v. RA needs bidirectional identity authentication with A mutually, and queries the user's info from the Users Manager, then creates right certificate for A.

vi. A can play the content by the special media player supporting DRM.

vii. The Check Agent can verify the copyright and trace the piracy behavior.

According to the analysis above, PCADRM system includes five modules: Content Packaging, Content Delivery, Right Management, Content Play and Copyright Verifying. The use case digraph is as follows.

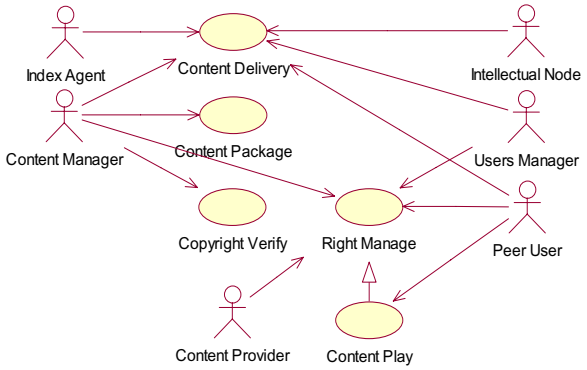

Fig. 2. The Use Case Digraph of PCADRM System.

B. The Characters of PCADRM System

Corresponding to the framework, we can conclude the characters of PCADRM system as follows:

(1) Security: The system security can be carried out from three aspects including content, user and right.

- The contents are packaged with special format through encryption and watermarking, and are granted special right.
- Users must register to login the system.
- The content must be played by special media player, through which, the content could be decrypted and the right could be parsed.

(2) Controllability

- Beforehand Control: the contents can be used with rights.
- Usage Control: the special media player must be used to play the content.
- Transmission Control: the encryption and IPsec are adopted.
- Post-Control: the extracting watermark and verifying copyright are used to monitor piracy behaviors.
- Access Control: the content delivery and right acquiring must be authenticated.

(3) Scalability: It can be realized from many aspects such as the functions, modularization, interfaces and rights expression language.

(4) Ability supporting behavior monitor and piracy tracing: The right certificate can be used to monitor and verify the user's behavior. And the piracy tracing can be implemented through watermark extracting and verifying.

III. CONTENT PACKAGING

The basic character of content security is CIA, namely Confidentiality, Integrity and Availability. The Confidentiality depends mainly on encryption technology. The Integrity is for ensuring the correction and veracity of content transmitted, which could be realized by Hash function and digital signature. The Access Control is used to ensure the content be sent to the prospective recipient but not illegal

ones.

In order to protect the media security, PCADRM system packages the media resources to the content object in predefined format with encryption algorithm and watermarking algorithm.

A. The Pattern of Content Packaging

There are two kinds of patterns of content packaging: centralized packaging and self-determined packaging. In the second one, the Content Manager will call the API of PA directly. So the interaction between PA and Content Manager has nothing to do with networks environment, and the implementation is simple and flexible.

The process of self-determined packaging in PCADRM system is presented in figure 3.

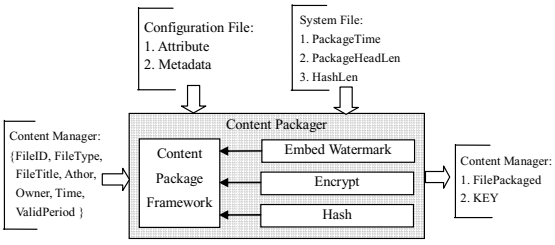

Fig. 3. the Process of Self-determined Packaging in PCADRM System.

Firstly, the Content Manager transfers information about the copyright and identification of media files to PA. Secondly, according to the encryption algorithm identification and watermarking algorithm identification, PA calls the relevant algorithm modules to create new media file packaged with P-DCF format criterion. Finally, the new media files and the KEY for content encryption are returned to Content Manager.

The digital watermarking algorithm is able to embed copyright information to the video frames extracted from the video streaming. So, $Media_W$, the new media with watermark is created:

$$Media_W = F\ (Media, Watermark)$$

The encryption adopts symmetrical AES algorithm that is used to encrypt $Media_W$ to ensure the confidentiality of content. The Hash function is realized by SHA-1 to abstract digest from the head file of media package, which can verify the integrity of content. The watermark will be extracted to verify copyright and trace piracy behavior.

B. The Format of Content Packaging

Before the content is packaged, other relevant information should be packaged together, such as file name, copyright, as well as some additional methods for the CIA of content. In PCADRM system, the content will be packaged is appended a head file including file head, attribute, metadata and Hash digest:

Content_Packaged = F (FileHead, Attribute, Metadata, HashDigest, Content)

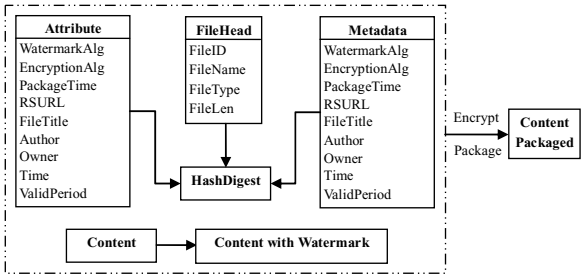

Fig. 4. The Format of Content Packaging.

The definition of Attribute and Metadata will conduce to the scalability of PCADRM system. The name of information is presented in Attribute list; however, the Metadata could be defined concretely according to practical applications. And the access address of Metadata can be computed from the original address and offset in Attribute list.

IV. P2P-BASED CONTENT DELIVERY

The architecture of P2P-based Content Delivery is designed as centralized directory service, which is carried out by Peer Agent of PCADRM system. The main functions of Peer Agent include:

i. Searching media resource according to the key words or key frame of video.

ii. P2P Downloading media resource from multipeers along the route elected on IPv6 networks.

iii. Delivering media resource to other peers.

iv. Updating the peer nodes information with Index Agent together.

v. Updating the peer nodes status with Intellectual Node.

In PCADRM system, all the interactions among nodes happen on IPv6 networks.

V. RIGHT AGENT WITH DISTRIBUTED-CENTRALIZED STRUCTURE

Right control is the core of DRM. Only legally authorized users could consume digital content correctly. In PCADRM system, RA combines the rights with digital contents, and controls the content access according to different rights.

A. The Structure of Right Agent

After Content Provider uploads media resource to Content Manager, the media resource and its future users must be authorized, which can be done through the interface provided by RA, and then the rights will be saved to database with the given data structure. While peer-user wants to browse the usable rights, RA can get the rights information from database and send to peer-user on the IPv6 network. If peer-user decides to purchase one or more of them, RA can create right certificate to peer-user when the bidirectional identity authentication between RA and peer-user is successful.

RA includes three modules: Rights Info Management, Right Certificates Management and Identity Authentication.

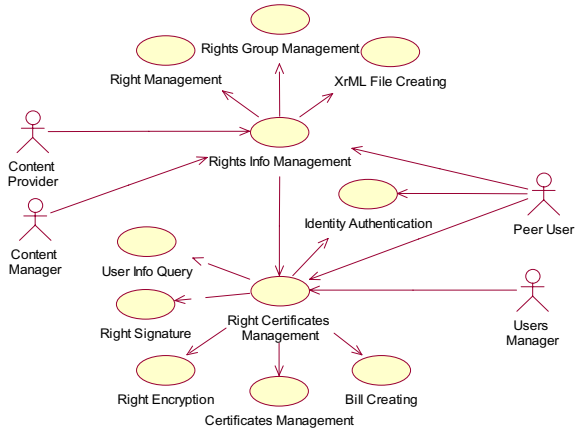

Fig. 5. The Structure of Right Agent caption.

The PCADRM system is designed for film and television industry. In order to make every content provider, for example TV station, control his own media resources and usage rights easily and securely, the structure of RA adopts the mix-mode combined distributed and centralized modes. Every TV station can build and control his own RA server that can deal with the right requests from peer-users located at same region, which could not only reduce the burden of networks bandwidth and server computing, but also provide the controllability. Moreover, right certificates and media files are stored and delivered separately, which will bring more flexibility to PCADRM system.

B. XrML-based Rights Info Management

There are three main functions in Rights Info Management: Right Group Management, Rights Management and XrML File Creating.

This module is designed as B/S structure, through which Content Provider can login the RA server by a browser easily. In contrast to C/S structure, in B/S structure, user needs not install special client software, and server software can be upgraded and maintained conveniently.

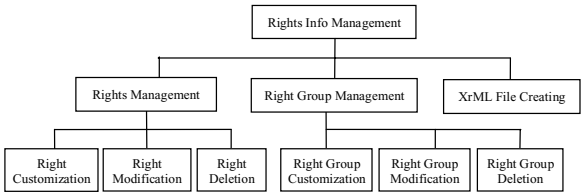

Fig. 6. The Modules of Right Info Management.

To make the right info management flexible and scalable, three configuration files are defined, which can be assembled and configured according to practical applications.

(1)RightGroupInfo={RightGroupID, RightGroupRegisterTime,RightGroupRegisterUser, RightGroupName,RightGroupType, RightGroupProperty, RightGroupPrice,RightGroupModifyTime, RightGroupModifyUser }

(2) RightMedaData = { Play, Copy, Rework, Print }

(3) RightsInfo={URI,FileName,RightsGroupID, RightMedadata,UserGroup,RightsRegisterTime, RightsRegisterUser, RightsModifyTime, RightsModifyUser, FileType, FileTimeStamp }

URI is the abbreviation of Unified Resource Identifier.

PCADRM system adopts XrML (Extensible Rights Makeup Language) to express and standardize rights, which includes four important elements: principle, right, resource and condition. On the basis of them, this module builds a template that contains the license metadata and semantic. The XrML template has a standard structure and syntax that is conduced to data interchange among systems with different structures. By the XrML template, XrML file can be created automatically.

C. PKI-based Bidirectional Identity Authentication

To ensure the security of rights purchase process, the bidirectional identity authentication based on PKI is needed between peer-user and RA. The public key of CA is 2048 bits, and the RSA public key of peer-user and RA is 1024 bits. Hash algorithm is SHA-1, and signature algorithm is RSA.

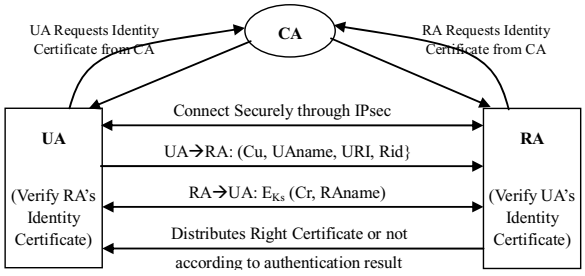

Fig. 7. PKI-based Bidirectional Identity Authentication.

In figure 7, the interaction between peer-user and RA is:

i. Connecting with IPsec: negotiating about the parameters of authentication and encryption, the pattern of authentication (in this system, AuMethod=PKI), and session key (Ks).

ii. UA→RA: E_{Ks} (Cu, UAname, URI, Rid)

Cu—Identity Certificate of User Agent, Rid—ID of Right selected by user.

iii. RA verifies peer-user's identity certificate.

iv. RA→UA: E_{Ks}(Cr, RAname), Cr—Identity Certificate of RA.

v. Peer-user verifies RA's identity certificate.

IPsec is compulsory protocol in IPv6 networks, which can provide secure service on IP layer through jointing two extendable message heads after main IP message head, one is AH (Authentication Header) to authenticate, the other is ESP (Encapsulating Security Payload) to group encrypt.

D. Right Certificate Creating and Management

When the bidirectional identity authentication is successful, RA will query Users Manager about whether the peer-user has

enough balance and credit to purchase right. If yes, RA will create right certificate and distribute it to peer-user through IPsec.

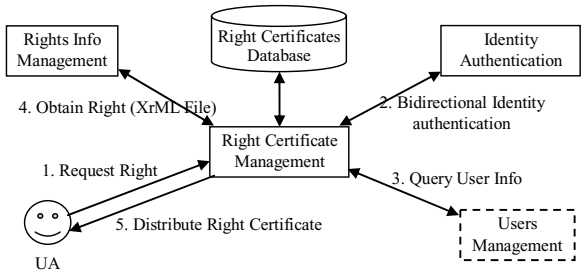

Fig.8. Right Certificate Creating and Management.

The XrML right file is obtained from Rights Info Management module, after that, right certificate will be created:

i. Signing XrML right file to ensure the integrity of right certificate:

$$SR = Sign_{Kr}^{-1}(Hash\ (R))$$

ii. Encrypting SR, XrML file and KEY to ensure the confidentiality of right certificate:

$$ER = E_{Ku}\ (R, SR, KEY)$$

After creating is successful, the right certificate is saved into database with the pattern {CerSN, UAname, IssueDate, Rid, URI}.

VI. Content Player supporting DRM

In PCADRM system, peer-user could play the media content downloaded only by a special player supporting DRM. This player's main functions include:

(1) Verifying right certificate

When peer-user received the right certificate from RA, the validity of right certificate needs to be verified. Firstly, (R, SR, KEY) = D_{Ku}^{-1}(ER), and D_{Kr}(SR), then judging whether D_{Kr}(SR) is equal to Hash(R). If the verifying is successful, the right certificate is saved in the peer node.

(2) Parsing right certificate

When peer-user begins to play the content, the player will check right certificate. If right certificate does not exist, peer-user will be inducted to purchase it. Otherwise, the player opens it and verifies detail rights in it.

(3) Parsing content

If the rights of content are verified successfully, the player will decrypt the content with KEY in the right certificate by AES algorithm.

(4) Playing content

The player can play the content after content parsing.

(5) Updating right certificate

The right certificate needs to be updated after the content is played.

VII. Conclusion

In this paper, we propose and implement a PCADRM system, a novel DRM system based on peer-to-peer networks for film and television industry. This system focuses on the content security, rights management and access control, which forms the whole trust model of PCADRM system. The content security is carried out through AES encryption, RSA signature, packaging and IPsec. The rights management with the distributed-centralized structure is more controllable and can reduce the burden of networks bandwidth and server computing. And the downloaded content can be played only with the rights control. The access control demands every user in the PCADRM system to register, and needs identity authentication during important interactions such as right purchasing. The implemented PCADRM system shows that it can provide a more robust Intellectual Property protection solution for P2P content delivery.

References

[1] Qiong Liu, Reihaneh Safavi-Naini, Nicholas Paul Sheppard, "Digital rights management for content distribution," The 2nd Australian Institute of Computer Ethics Conference (AICE2000), Canberra, 2000.

[2] Guofei Gu, Bin B. Zhu, Shipeng Li, Shiyong Zhang, "PLI: a new framework to protect digital content for P2P networks," Lecture Notes in Computer Science, 2003, Vol.2846: 206-216.

[3] YU YinYan, TANG Zhi, "A survey of the research on digital rights management," CHINESE JOURNAL OF COMPUTERS, 2005, 28(12).

[4] Tetsuya Iwata, Takehito Abe', Kiyoshi Ueda, Hiroshi Sunaga, "A DRM system suitable for P2P content delivery and the study on its implementation," The 9th Asia-Pacific Conference, 2003, Vol.2: 806-811.

[5] Bill Rosenblatt. (2003). Integrating DRM with P2P networks. Available: http://www.drmwatch.com/resources/ whitepapers/article.php/3112631.

[6] Paul Judge and Mostafa Ammar, "The benefits and challenges of providing content protection in peer-to-peer systems," In: Virtual Goods 2003 - International Workshop for Technology, Economy, Social and Legal Aspects of Virtual Goods: 22. - 24. May; Ilmenau, Germany.