A DRM ARCHITECTURE FOR MANAGEABLE P2P BASED IPTV SYSTEM

Xiaoyun Liu[1], Tiejun Huang[2], Longshe Huo[2], Luntian Mou[1]

[1]Graduate University, Chinese Academy of the Sciences, Beijing, China 100039
[2]Institute of Digital Media, Peking University, Beijing, China 100871
{xyliu, tjhuang, lshuo, ltmou}@jdl.ac.cn

ABSTRACT

With the improvement of network bandwidth, multimedia services based on streaming live media have gained much attention recently, among which IPTV has become a hot topic. After emergence of Peer-to-Peer (P2P) technology, P2P based IPTV systems are deployed widely. However, there exists a huge challenge, which is how to manage content. Digital Rights Management (DRM) is such a system that includes encryption and other technologies which can control the usage and redistribution of the digital contents. In this paper, we first review the related works in this area and analyze the DRM requirements. Then we propose a DRM architecture for a manageable P2P based IPTV system. In our architecture, we also present content encryption scheme and content authentication scheme.

1. INTRODUCTION

With the improvement of broadband IP network, multimedia services based on streaming live media have gained much attention recently, among which IPTV has become a hot topic [1].

A challenge of IPTV is how to distribute programs to millions of end-users simultaneously, which requires huge network bandwidth. IP multicast may be a choice. However, due to the practical issues of routers, it has not been widely deployed. Peer-to-Peer (P2P) technology is a highly efficient method for multimedia streaming. P2P based IPTV system does not rely on dedicated application-level multicast servers. Instead, each IPTV client is potentially a server, receiving contents from up-level peers and redistributing them to down-level peers, thus alleviating the pressure of multimedia server.

However, nowadays there is still a critical problem within the system: most of the P2P based IPTV systems (such as PPLive[11]) do not take into account content management. Digital content can be copied or redistributed without any restriction, which of course is undesired. Therefore a content management system is required for the practical deployment of P2P based IPTV. Digital Rights Management (DRM) is such a system that includes encryption and other technologies which can control the usage and redistribution of the digital contents.

In this paper, we propose a DRM architecture for manageable P2P based IPTV system after a brief introduction of some related works. The rest of this paper is organized as follows: Section 2 reviews the related works in this area; Section 3 analyzes the DRM requirements for the system; Section 4 gives the architecture and discusses the relative schemes; finally Section 5 concludes this paper.

2. RELATED WORKS

In recent years, the topic of DRM has gained more and more popularity. With the P2P technology based applications widely deployed, the topic of DRM in P2P systems is of great importance and many researches have been done in this area.

Androutsellis-Theotokis et al. [2] gives an overview of the P2P content distribution technologies and then deals with the security issues characteristic of P2P content distribution systems. These issues include secure storage, secure routing, access control, authentication, and identity management.

For multimedia content distribution in P2P networks, Chu et al.[3] proposes a mobile DRM system and business model, which utilize client side application and tamper-resistant hardware to enforce digital rights. The approach in this system is based on peer side hardware authentication, which is similar to the Trust Computing (TC) technologies. Similarly, Zhang et al.[4] and Balfe et al.[5] use the TC technologies to enhance or provide security for P2P systems.

Iwata et al.[6] discuss the DRM system applicable to P2P content sharing and focus on DRM methods and DRM function assignments suitable for P2P content delivery. Balfe et al.[7] classify existing researched approaches into three types: conventional Server-Client based DRM architecture, distributed P2P based DRM architecture and semi-distributed P2P based DRM architecture. After comparing the pros and cons of these architectures, they propose a new type of DRM applied P2P system architecture that still keeps existing P2P system's advantage.

3. DRM REQUIREMENTS FOR P2P IPTV

A DRM architecture should provide security for P2P based IPTV system while maintaining advantages of P2P technologies. From this aspect, current three architectures mentioned above have their own advantages and deficiencies. Conventional Server-Client based DRM architecture has good security characteristics; however the DRM server in the system may be the bottleneck of the whole system, which cripples the P2P's advantages. Distributed P2P based DRM architecture doesn't have a DRM server and have nearly all of the DRM functions assigned on the peer node (Super Node). However this distribution affects the security adversely. Semi-distributed P2P based DRM architecture falls between them.

TC technologies are effective methods to provide security in P2P systems. However, at present TC technologies always rely on hardware to provide security, and there is no such hardware on the client side of most IPTV systems. It is still a long way before TC technologies can be deployed in practical DRM systems.

Obviously a P2P system should also provide other security mechanisms such as access control, super-distribution, authentication etc.

To achieve access control and super-distribution, the content delivered between peers should be encrypted. Then the encrypted content can be freely distributed on the Internet and when the end-users get it, only the authorized ones can access that content.

Authentication is also required. From the perspective of users, they often want guarantees of integrity and sometimes non-repudiation on the received data. On the other side, the content provider does not want to be impersonated by another party. The source authentication is also necessary to prevent malicious attacks which frequently occur in many broadcast networks.

To address these problems, in this paper we propose a new DRM architecture which considers both data encryption and authentication schemes, and can guarantee both security and P2P advantages.

4. PROPOSED ARCHITECTURE

As described in Section 3, the more distributed the system is the less reliable the security will be. A tradeoff should be made between how distributed the system is and how secure it can be. In P2P based IPTV system, semi-distributed P2P based architecture is a good choice, in which critical DRM functions, such as License and Key distribution, exist in the separated DRM server while all others lie in peer nodes. In this section, we propose a new semi-Distributed P2P based architecture (see Fig. 1), and discuss the related encryption and authentication schemes.

4.1. Architecture overview

In this architecture, we introduce a kind of special Super Node—MARS (Multimedia Application Routing Server), which is used at the application-level for routing multimedia RTP packets and performing some DRM functions such as packet authentication, peer management, and etc.

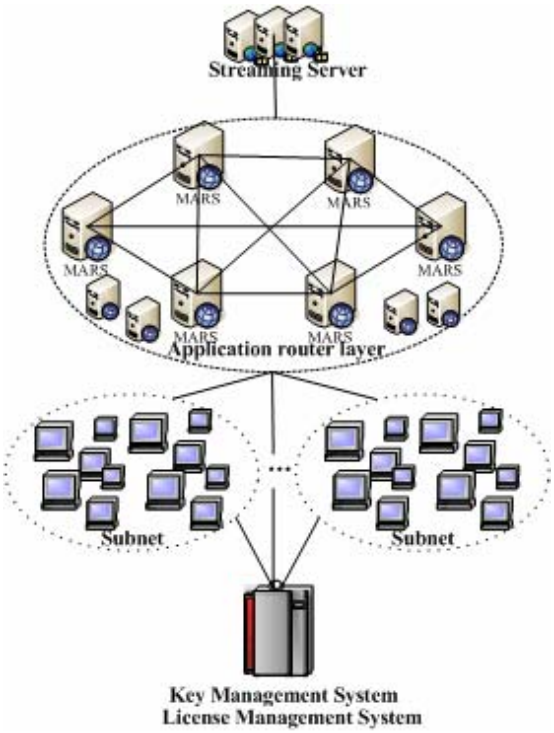

Figure 1. Architecture overview

Our P2P based IPTV system is comprised of two levels of P2P networks. The first level of P2P network is made up of MARS. On this level each MARS is a Super Node and all of the multimedia RTP packets should be filtered through MARS. It checks the integrity of the Multimedia datagrams and authenticates their sources to assure that they are from legitimate content provider. It is also responsible for the management of the peers which are connected to it. The second level is made up of subnets which are composed of millions of end-users. Each subnet is an independent P2P network and connected to the upper-level MARS network. End-users in subnets do not need to authenticate the multimedia RTP packets, since all the packets from the streaming server would be routed through MARS.

The architecture in Fig.1 also contains Key Management System (KMS) and License Management System (LMS), which are two integral parts of a complete DRM system. In this P2P based architecture, the separated KMS and LMS server will be the bottleneck of the whole system. The performance of the system will become unacceptable if lots of end-users frequently request for Key or License at the same time. In the following subsection we propose a reasonable scheme to mitigate this bad effect.

4.2. Encryption scheme

To achieve security requirement mentioned in section 3, the multimedia packet transmitted between peers should be encrypted to prevent illegal copy and redistribution. Only legal end-users, who get the Keys or License from KMS and LMS, can access the content legitimately.

Most existing DRM systems apply encryption method on the whole content, and so modify its file format. However, the Streaming Sever sends data according to file format of the content. To preserve file format of the content, we only need to encrypt the payload of RTP packet.

To facilitate encryption on the packet payload, ISMA (Internet Streaming Media Alliance) DRM[10] proposes a new payload format which is based on RTP payload format defined in mpeg4-generic [RFC 3640]. Fig. 2 shows data sections within an mpeg4-generic RTP packet. The new payload format inserts cryptographic metadata at the beginning of the AU header section. Fig. 3 shows the inserted fields (Note that in Int(n), n is a bit count). AU_is_encrypted is a single bit field to signal selective encryption: 1 signals that corresponding AU is encrypted; 0 means not. IV contains all the needed information to decrypt each AU contained in the packet. Key_indicator indicates which key used to encrypt (decrypt) this AU.

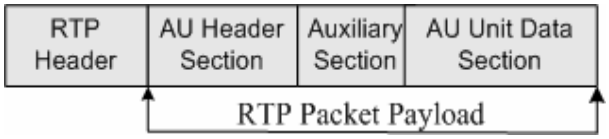

Figure 2. An mpeg4-generic RTP packet

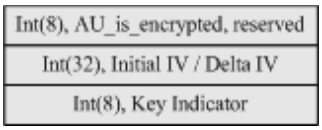

Figure 3. Added fields

ISMA DRM is an outstanding scheme for streaming media on the internet, but it is not designed for P2P situation. For security consideration, its Key_indidator should be updated regularly, which will bring heavy burden to the KMS and LMS server in P2P system. So it still doesn't solve the bottleneck issues caused by the separated DRM server. To alleviate the bottleneck effect, we propose an improved scheme based on the ISMA DRM. Fig. 4 presents our added fields. Our scheme uses a two-level key structure with MasterKey on the first level and SaltKey on the second level. MasterKey is issued by KMS and LMS server and SaltKey is distributed together in RTP payload. Content Encryption Key (CEK), used to encrypt RTP payload, is computed from MasterKey and SaltKey. By frequently changing the SaltKey in the packet, we can reduce the frequency of MasterKey updates to alleviate the pressure on KMS and LMS server. In this way, our scheme mitigates the bottleneck effect of the whole system.

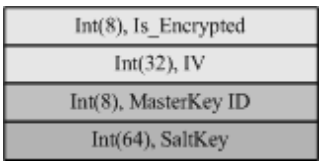

Figure 4. Our added fields

Note that in the new payload format only AU data section can be encrypted since AU header section contains the decryption information. End-users should send requests to KMS and LMS to obtain MasterKey or License according to the MasterKey ID when they receive a packet. Therefore, it assures that only authorized end-users can access the content and use them under specified rights.

4.3. Authentication Scheme

Manageable P2P based IPTV system must authenticate the source of content to prevent illegal packets from appearing on the Internet. In this architecture, we assign this task to MARS. In some sense, MARS is a monitor which supervises all the multimedia packets over the P2P based network.

A straightforward stream authentication method would use a digital signature on each packet of the stream. But the resulted overhead would be high, both in terms of the time and bandwidth. Several schemes have been proposed by researchers. In general, these schemes can be divided into two categories. The first category is to mitigate the overhead by amortizing a single signature over several packets, e.g. [12,13]. But most of IPTV systems do not use reliable transport layer and some packets may be lost during transmission. Some schemes of this catalog introduce enough redundancy in the authentication information that even if some packets are lost, the required authentication information can be recovered. However, they are still not robust to packet loss and the redundant authentication information also increases the bandwidth overhead. The second category is to use symmetric algorithm to authenticate packets [14,15]. This category mainly uses symmetric cryptography and time-delayed key disclosure to achieve the required asymmetry property. It requires receivers be synchronized with the sender's clock. This category can be used in multicast situation but it is not suitable for P2P based environment, since when packets are redistributed to another peer the asymmetric property may don't exist any more.

To overcome the deficiencies of the above schemes, we suggest our approaches. In our scheme, to improve the robustness against packet loss, content Providers sign every packet that they sent to P2P network. However, the overhead caused by signature still exists. To mitigate the bandwidth overhead, among several Public-Key Cryptographies we adopt ECC[16] due to its acceptable overhead. Our scheme selects ECC-192 as the signature algorithm, which can provide higher security level than

RSA-1024 while the length of its signature is 48 bytes compared to 128 bytes of RSA-1024. Another problem mentioned above is computation cost. In our system the authentication process occurs at the Super Node - MARS which is transparent to end-users. The computation overhead then is imposed on MARS and end-users are spared. To improve the performance of MARS, the verification procedure can be implemented by dedicated hardware and selective packet authentication or verification may be adopted.

Figure 5 shows the packet format with authentication information.

Figure 5. Packet format with authentication tag

The authentication process is carried out as follows: First, we apply the HMAC-SHA1[17] to the whole RTP packet and get the HMAC output. Second, sender encrypts the output bits using ECC algorithm and gets an authentication tag. The authentication tag is then added at the end of the RTP packet when it is being sent. When the packets arrive at MARS, MARS will verify them. Only authenticated packets will be transmitted to subnets by MARS and all others would be discarded. Therefore, it assures that only legitimate packets appear on subnets.

5. CONCLUSION

In this paper, we review the related works about DRM on P2P networks and analyze the DRM requirements for P2P systems. Based previous works, we propose a new DRM architecture for a manageable P2P aided IPTV system and present content encryption scheme and content authentication scheme deployed in the system.

6. ACKNOWLEDGMENT

This work was done when the author was with Peking University, and was partially supported by the Key Technologies R&D Program of China under grant No. 2006BAH02A10.

7. REFERENCES

[1] Benjamin Alfonsi, "I Want My IPTV: Internet Protocol Television Predicted a Winner", IEEE Distributed Systems Online, vol. 6, no. 2, 2005.

[2] Stephanos Androutsellis-Theotokis and Diomidis Spinellis, "A survey of peer-to-peer content distribution technologies", ACM Computing Surveys, 36(4):335–371, December 2004

[3] Chu C.C., Su X., Prabhu B.S., Gadh R., Kurup S., Sridhar G. Sridhar V., "Mobile DRM for multimedia content commerce in P2P networks", Consumer Communications and Networking Conference, 2006 3rd IEEE Volume 2, 8-10 Jan. 2006 Page(s):1119 – 1123.

[4] Xinwen Zhang, Songqing Chen, Ravi Sandhu, "Enhancing Data Authenticity and Integrity in P2P Systems," IEEE Internet Computing, vol.09, no.6, pp. 42-49, Nov/Dec, 2005.

[5] Shane Balfe, Amit D. Lakhani, Kenneth G. Paterson, "Trusted Computing: Providing Security for Peer-to-Peer Networks," p2p, pp. 117-124, Fifth IEEE International Conference on Peer-to-Peer Computing (P2P'05), 2005.

[6] Iwata T., Abe T., Ueda K., et al. "A DRM System Suitable for P2P Content Delivery and the Study on Its Implementation", The 9th Asia-Pacific Conference on Communications, 2003, pp. 806-811.

[7] Balfe S., Lakhani A.D., Paterson K.G., "DRM Enabled P2P Architecture", Peer-to-Peer Computing, 2005. Fifth IEEE International Conference on 31 Aug. 2 Sept. 2005 Page(s):117 - 124

[8] Feng Cao, David A. Bryan, Bruce B. Lowekamp, "Providing Secure Services in Peer-to-Peer Communications Networks with Central Security Servers," aict-iciw, p. 105, Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT-ICIW'06), 2006.

[9] Eugene T. Lin, Gregory W. Cook, Edward J. Delp, Paul Salama, "An Overview of Security Issues in Streaming Video," itcc, p. 0345, International Conference on Information Technology: Coding and Computing (ITCC '01), 2001.

[10] Internet Streaming Media Alliance, www.isma.tv

[11] PPLive, www.pplive.com

[12] A. Perrig, R. Canetti, J. D. Tygar, andD. Song, "Efficient authentication and signature of multicast streams over lossy channels", Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 56 – 73, May 2000

[13] C. K. Wong and S, S. Lam. "Digital signatures for flows and multicasts", IEEE/ACM Transactions on Networking, 7(4):502–513, 1999

[14] A. Perrig, R. Canetti, J. Tygar and D. Song, "the TESLA Broadcast Authentication Protocol", RSA CryptoBytes, 5, Summer 2002

[15] A. Perrig, R. Canetti, J. Tygar and D. Song, "Efficient and Secure Source authentication for multicast", Network and Distributed System Security Symposium, NDSS'01, Feb. 2001

[16] ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve, Digital Signature Algorithm (ECDSA), 1999.

[17] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997