Improved Threshold Secret Sharing Distributed License Authorization System

Hongmin Jiang, Ying Li
School of Computer Science
Communication University of China
Beijing, China
zoray@163.com

***Abstract*—The demand for digital rights management (DRM) in P2P mode is increasing accordingly along with rapid popularity of the P2P networks. The key points in DRM are the management and issuance of digital content licenses. The traditional centralized authorizations have certain limitations in security and efficiency. This paper presents an improved distributed license authorization system which divides P2P network nodes into six kinds of roles in accordance with their functions. The role of authoritative peer is introduced in order to lighten the burden on the content provider existing in previous systems. The adoptions of threshold secret sharing mechanism and independent synthesis peer in delivering and synthesizing the digital content licenses effectively improve the security of the license in the P2P network environment.**

Keywords-P2P; DRM; RSA; threshold secret sharing mechanism;

I. INTRODUCTION

Accompanied by the rapid development of the computer industry, P2P network quickly caught the attention of various parties with its direct, fast, flexible digital content transmission advantage. At the same time, the development of P2P technology has also given rise to a series of disputes and problems, mainly concentrated on the severe impact on the existing copyright system of network resources. On account of this situation, people put forward a lot of superior digital rights management frameworks based on P2P mode, whichsoever kind of framework gave sufficient attention to the generation and transmission of digital content license.

In the traditional digital copyright management authentication systems[1][2], the digital content licenses are provided by a special Certificate Authority (CA) center. When the users need to use the digital content, they need to apply to CA for permission. After the user's authentication and authority are confirmed by CA, it will produce a corresponding content digital license which is supposed to return to the user. It is called centralized authorization system[3][4].

S. Q. Xiao et al proposed a trust scheme based on digital rights management (TSDRM) model[5][6], brought into the Authoritative Peer (AP) to save and calculate the secret share which effectively released the CA license application pressure. After content provider released the encrypted license by public key based on RSA[7] encryption mechanisms then shared the private key in APs. The user needed to collect k or more parts of secret shares from Aps to recombine the private key which is used to decrypt the encrypted license. The threshold secret sharing mechanism also increases fault tolerance and security. Because AP was responsible for secret distribution and participated in the final license calculation, in the large-scale of P2P network, AP network loads would increase obviously and could be attacked, causing the license distribution or the final synthesis failure. H. Zhao et al proposed a new threshold secret sharing (TSS) distributed license authorization system[8], which divided P2P network nodes into four kinds of roles according to their performance, and adopted the Shamir threshold secret sharing mechanism[9] to share the license secrets. In this system the distribution and calculation of the license secrets were designed on different kinds of network nodes. License was synthesized in the super peer, due to which the problems existing in TSDRM were effectively solved. However, distributed license synthesis was concentrated into a single optimal super peer, for large-scale of P2P networks, in the same P2P network, short-term inside node was not obvious. The optimal super peer being illegally breached the risk, once breached the license should be illegally stolen. Meanwhile, when the content provider conducted secret sharing of different content recourses, the network loads on the content provider should significantly increase.

In order to prevent the optimal super peer from exposure and lighten the network loads on the content provider, this paper proposes an improved license authorization system based on TSDRM and TSS distributed license authorization system, which effectively improves the license security and significantly and releases the network burden on the content provider. This system will be more suitable for the current P2P network environment.

II. IMPROVED THRESHOLD SECRET SHARING DISTRIBUTED LICENSE AUTHORIZATION SYSTEM

The threshold encryption system refers to saving the secret data in the following way: first of all, the secret is split into a number of secret shares; then distributes the secret shares to a plurality of network nodes. When the number of network nodes is less than a given threshold value, the secret is broken, no information of the original secret will be exposed. If the shared secret reconstruction is requested and the count of network nodes which have the secret share is not less than the threshold number, the system will recover the original secret information.

The nodes in the P2P network are divided into six kinds of roles in accordance with their function:

Published by Atlantis Press, Paris, France.

- User: requests, downloads, the decrypts content resources peer node;
- Content distribution Peer (P): composed of distributed content distribution systems, secondary encryption of network resources, and provides users with download resource nodes;
- Authoritative Peer (AP): saves the grouped license key seed (GLKS) which is divided by content provider. Achieves and maintains grouped license key seed threshold secret sharing, and distributes the encrypted content resources slice, single authoritative peer only knows part of the license key seed.
- Grouped License Issuer (GLI): special node with distributing grouped license authorized function, can share the grouped license key seed which is provided by Authoritative Peer.
- Grouped Super Peer (GSP): composed of the grouped license authorized and synthesis system. Updates and maintains distributed grouped license authorized node index table <CID, GLI_{i1}, GLI_{i2}, …, GLI_{in}>, locates the grouped license issuer and synthesizes the grouped license key seed;
- Synthesis Peer (SP): collects various subgroups of grouped license key seeds synthetized by optimal grouped super peers provided by content publisher, then completes the final synthesis and issues the license to user.

A. *Improved distributed Threshold Secret Sharing license system architecture and work flow*

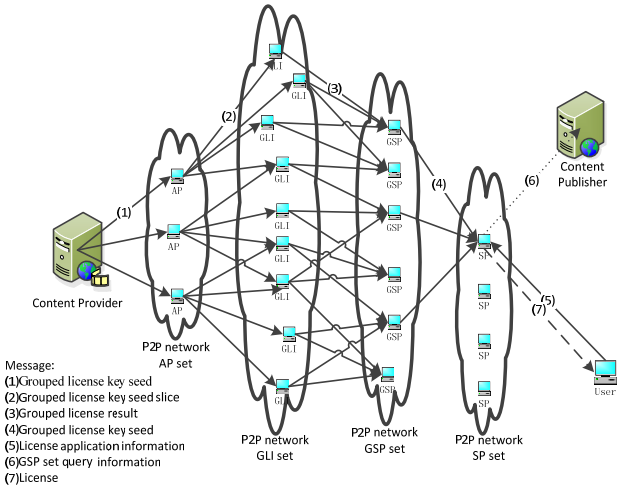

Figure 1. Improved distributed threshold secret sharing license system framework

Its workflow is as follows:

1) Content provider selects a group of higher authority nodes as authoritative peer set, and divides the license key seed into groups, then respectively passes the grouped license key seeds to the appropriate authoritative peers.

2) Authoritative peer generates the grouped license after processing grouped license key seed with content provider's public key (PPK) which is generated by the RSA encryption mechanism, then shares the grouped license key seed in multiple grouped license issuer set of GLI_{i1}, GLI_{i2}, …, GLI_{in}(i=1,2,…) by threshold secret sharing mechanism.

3) Authoritative peer generates a distributed grouped license authorization index table <CID, GLI_{i1}, GLI_{i2}, … , GLI_{in}> (i = 1,2, ...) which is sent to multiple grouped super peers to provide distributed grouped license authorized services for the final synthesis peer.

4) When the grouped super peer receives distributed grouped license authorization index table, it needs to be registered with the content publisher.

5) According to the certain strategy, the user selects a set of peers from the P2P network as synthesis peer set. When the user wants to use some content resouses, user needs to send a content resource license application to the optimal performance one, which is treated as the final synthesis peer to synthesize the license, and the rest of the synthesis peers are reserved for future use.

6) The synthetic peer sends query information to the content publisher to get the grouped super peer set of the content resource.

7) Content publisher selects a set of super peers as the distributed grouped license authorized peer set from the grouped content resources super peer sets of each group in accordance with certain policies, then sends grouped license authorization requests to the optimal performance grouped super peer in each group, the rest of the grouped super peers are reserved for future use.

8) According to its distributed grouped license authorized node index table <CID,GLI_{i1},GLI_{i2},…,GLI_{in}> on the grouped super peer, the selected one will inform each grouped license issuer to start the grouped license distributed generation action.

9) Each grouped license issuer will return the generated grouped license to the corresponding grouped super peer, then grouped super peer generates the grouped license key seed, which will be sent to the final synthesis peer.

10) After the optimal grouped super peer of each group of the content resources sends the grouped license key seed to the final synthesis peer, the license will be presented to the user after generated based on the user's identity and permissions license.

B. *Secret sharing*

1) After completion of the initial encryption of the content, the content provider generates a public key(PPK) and private key(PSK) based on RSA encryption mechanisms, then divides the license key seed into equal groups of $GLKS_1$,$GLKS_2$…$GLKS_m$, which are passed to authoritative peers respectively.

2) Authoritative peer generates the grouped license(*gl*) after processing grouped license key seed with content provider's PPK.

3) Authoritative peer constructs (*k*, *n*) threshold secret sharing polynomial:

$$f(x) = PSK + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \bmod p \quad (1)$$

PSK is a content provider's private key which is generated by RSA encryption mechanism.

4) Authoritative peer transmits secret key shared slice S_i via a secure channel to the *n*-th grouped license issuer. S_i is associatedt with their identification information *i*:

$$S_i = f(i) \bmod p \tag{2}$$

5) Authoritative peer generates validation message parameters *g*, which's length is less than the length of *n*, then broadcasts the secret sharing polynomial coefficient evidence $\{g^{a_0}, g^{a_1}, \ldots, g^{a_{k-1}}\}$ to grouped license issuers.

6) Grouped license issuer uses the following equation to verify the receipt of shared secret slice's facticity and availability:

$$g^{s_i} = g^{a_0} \cdot (g^{a_1})^i \cdot \ldots \cdot (g^{a_{k-1}})^{i^{k-1}} \bmod p \tag{3}$$

The secret sharing as shown in the following Fig. 2:

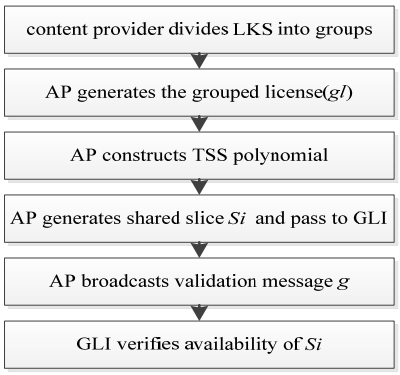

Figure 2. Secret sharing workflow

C. Synthesis of the license

According to the optimal strategy, the user locates the best performance synthesis peer; The selected synthetic peer sends query information to the content publisher to get the grouped super peer set of the content resources; Content publisher selects a set of super peers as the distributed grouped license authorized peer set from the grouped content resources super peer set of each group in accordance with certain policies, then sends grouped license authorization requests to the optimal performance grouped super peer in each group; According to distributed grouped license authorized node index table, the selected grouped super peer informs each grouped license issuer to start grouped license distributed generation action.

1) Each grouped license issuer uses the following equation to calculate the partial lincense results gl_i:

$$gl_i = (gl)^{s_i} \bmod p \tag{4}$$

2) Each grouped license issuer generates a random number *u*, then calculates as follows:

$$F_1 = g^u \tag{5}$$

$$F_2 = (gl)^u \tag{6}$$

$$r = u - c \cdot S_i \tag{7}$$

$$c = hash(g^{s_i}, gl_i, F_1, F_2) \tag{8}$$

The calculation results gl_i, F_1, F_2, and *r* are returned via a secure channel to the distributed grouped super peer.

3) The grouped super peer calculates the results based on secret sharing polynomial coefficients evidence:

$$g^{s_i} = g^{a_0} \cdot (g^{a_1})^i \cdot \ldots \cdot (g^{a_{k-1}})^{i^{k-1}} \bmod p \tag{9}$$

Then it uses the parameters gl_i, *F1, F2* by (8) to calculate number *c*; certifies receipt grouped license gl_i, by equation $g^r \cdot (g^{s_i})^c = F_1$ and equation $gl^r \cdot (gl_i)^c = F_2$; Repeats the above steps until grouped super peer received a *k*-effective part of the grouped license. If the grouped license number received within a predetermined time is less than *k*, the licensing request is failed; the user needs to relocate other grouped super peer to calculate again;

4) Grouped super peer uses k-effective part of the grouped license to calculate grouped license key seed which is equal to the corresponding authoritative peer.

$$GLKS = \prod_i (gl_i)^{\omega_i(0)} = (gl_i)^{\sum_i S_i \omega_i(0)}$$
$$= (gl)^{PSK} = ((GLKS)^{PPK})^{PSK} \bmod p \tag{10}$$

and $\omega_i(x) = \prod_{j=1, j\neq i}^{k} \frac{x - i_j}{i_i - i_j}$.

5) The optimal grouped super peer of each group of the content resources sends the grouped license key seed to the final synthesis peer, the license will be presented to the user after generated based on the user's identity and permissions license.

The synthesis of the license as shown in the following Fig. 3:

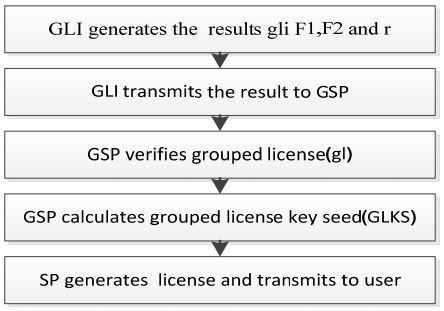

Figure 3. Synthesis of the license

III. CONCLUSION

An improved distributed license authorization system is presented in this paper. The new architecture combines the advantages of both TSDRM and TSS, and eliminates the limitations of a single architecture. The system's security has been further improved. The introduction of AP lightens the network loads on the content provider and single AP only knows part of the license in order to avoid the exposure of license. The adoptions of threshold secret sharing mechanism and independent synthesis peer in delivering and synthesizing the digital content licenses effectively improve the security of the license in the P2P network environment; meanwhile the adoption of synthesis peer prevents the optimal super peer from exposure. However, as to the model, there are still some areas of improvement, such as the strategy for updating different peer, and efficiency. While the increase of the role will certainly increase the amount of message communication, the method to reasonably manage these messages is needed. We will focus on these topics in the future-research.

ACKNOWLEDGMENT

The work is supported by National Key Technology R&D Program under Grant 2012BAH02F04.

REFERENCES

[1] B. Rosenblatt, W. Trippe, and S. Mooney, "Digital rights management. Business and Technology," New York: M&T Books, 2002, pp. 83-84.

[2] Kamvar SD, Schlosser M T. EigenRep, "Reputation Management in P2P Networks,".Proc. of the 12th Int'l World Wide Web Conf.New York, USA: ACM Press, 2003.

[3] Okamoto T, Pointcheval D. The Gap-problems: A New Class of Problems for the Security of Cryptographic Schemes[C].Proc. Of Public Key Cryptography Conference. Berlin, Germany: Springer-Verlag, 2001.

[4] R.Iannella, "Digital Rights Management (DRM) Architectures," D-Lib Magazine, vol. 6, 2001, pp. 207 ～216.

[5] S. Q. Xiao, Z. D. Lu and H. F. Ling, "A Trust-Scheme-Based DRM Model for P2P System," Computer Research and Development, vol. 44, 2007, pp. 567-573.

[6] L. Li, "Research on The P2P environment DRM model," Dalian University of Technology, China, 2008.

[7] R. Rivest, A.Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, Feb. 1978, pp. 120-126 .

[8] H. Zhao, "Based on P2P Streaming Media Digital Rights Management," Chongqing University, China, 2008.

[9] A. Shamir, "How to Share a Secret," Communications of the ACM, vol. 22, 1979, pp. 612-613.