A Token-based Authorized File-Sharing Protocol for BitTorrent-like P2P Systems

Hung-Wen Yang[1], Chou-Chen Yang[2] , Yi-Ju Lin[2] and Woei Lin[1]
1 Department of Computer Science and Information Engineering, National Chung Hsing University
2 Department of Management Information Systems, National Chung Hsing University
250 Kuo Kuang Rd., Taichung 402, Taiwan R.O.C.
{hwyang.tw@gmail.com*, cc.yang@nchu.edu.tw, g9829003@mail.nchu.edu.tw, wlin@cs.nchu.edu.tw}

Abstract- **In recent years, more and more people use Internet and with the improvements of communication technology, information-sharing trends has surged over Internet. Bit-Torrent is a well-known P2P application used for distributing large amounts of data and exchange digital content with high efficiently and scalability. Unfortunately, many users do not get authorization but transmit files through Bit-Torrent illegally. The piracy problems become a very serious issue because the digital contents can be copied and redistributed easily through P2P network without license owners' authorized. For this reason, digital rights management (DRM) is considered as a general preventive measure to avoid copyright infringement. However, a conventional DRM system implementation on distributed P2P network would be quite difficult. Therefore, we propose an efficient DRM model on P2P network that to prevent violation of copyrights for digital content owners and to provide more attractive motivation for users.**

I. Introduction

With the great development of network technology, more and more people join Internet to request for data. To use network bandwidth adequately, people need an efficiently interchangeable platform for speeding the file sharing and exchanging. Presently, the P2P architecture is the main method to distribute data flow and use network bandwidth more efficiently and scalability. Peer-to-peer networks have become the main stream of file-sharing platform by means of its distribution features to overcome the bottleneck problem in traditional client-server architecture. But the copyright infringement becomes a serious problem, due to these convenient features, more and more people use them to transmit unauthorized files. The piracy issue seriously hurts license owners' deserved profits and potential market. For this reason, digital rights management (DRM) is considered as a general preventive measure to avoid copyright infringement. Recently, the concept of Digital Rights Management (DRM) was proposed [1-7]. The major purpose of the DRM is to keep the intellectual property from being redistributed without the consent of the owner. The DRM system deals with the process of the digital contents including protection, distribution, and authorization. With the help of DRM technology, intellectual property is protected by data encryption so that it can only be accessed by authorized users without limitless distribution. However, a conventional DRM system is only suitable for client-server architecture, and its implementation on distributed P2P network would be quite difficult. Although some researchers have proposed some systems combining DRM with P2P network, the effect is limited. Therefore, for constructing a reliable transaction platform, we construct a DRM business model on P2P network that to prevent violation of copyrights for digital content owners and to provide more attractive motivation for users.

In [4], it presented a secure transaction platform that protects digital content copyright and allows all P2P users legally exchange files. In [5], Chen et al. came up with a DRM business model for BT system based on Diffie-Hellman key agreement protocol [6], and improved Zhang's mechanism [7]. Although, Chen et al.'s scheme can protect every piece of file and license to defense illegal access. Even an attacker gets all pieces of file and license; the attacker can't decrypt and play the file. But Yang et al. [8] pointed out there are still some security and commercial issues in their scheme and proposed another business model considers copyright protection and secure transaction based on P2P networks. In this paper, we proposed a new business model that considers copyright protection, secure transaction, technological implementation feasibility, and consumer's psychological cognition. We inherit the concept of [4] and enhancement of Yang et al.'s scheme [8], which is more suitable for practical P2P environments.

The rest of this paper is structured as follows: A brief review of related works is illustrated in section 2. A token-based authorized file-sharing protocol for P2P Systems is proposed in section 3. The related analysis of our proposed scheme is presented in section 4. Finally, the conclusion is in the last section.

II. Related Works

A. P2P Networks

With the growing development of P2P technology, file sharing on the Internet becomes easier. In the P2P network, everyone not only be a client to download file, but also a server to provide their bandwidth. Regarding the different scheme, P2P networks can be divided into centralized P2P system, decentralized P2P system and hybrid P2P System. The centralized P2P system must have a central index server to manage and record IP address of peer and where the file is, such as Napster [9]. Comparing with centralized P2P system, there is no central server in the decentralized P2P system and it is based on the distributed hash table (DHT) such as Chord [10] and Pastry [11]. Each peer can join and leave freely. When a requester wants to search a file, and then sends requests to its neighbor peers, these neighbor peers will determine whether it contain the file. Hybrid P2P system is kind of system combines the advantage and feature with above two types of P2P system. This system will select some peers which have strong computation capability and bandwidth to be a super peer. The super peers need to serve the local peers in a range. Each super peer and its managed local peers compose a centralized P2P system, and these P2P systems compose decentralized P2P system to become a hybrid P2P system, such as eMule and BT.

B. Bit-Torrent (BT) File-sharing System

BT system is a peer-to-peer file sharing protocol used for distributing large amounts of data. BT protocol can be used to reduce the server and network impact of distributing even large files, because of the system will divide a file into many pieces, everyone can download these pieces to assemble the original file, and when they download these files, they also can be a server to provide these files. In BT system, a peer who wants to share a file first builds a small torrent file and distribute by conventional ways. Peers willing to get the file initially download the torrent file. The torrent file contains the meta-information about the file such as the address of the tracker site and the information about the file pieces. A tracker site is a web server that maintains a list of the current peers that can be contacted. Once the peers receive the list of peers, it can establish TCP connections with some of them to download data. As a peer receives a new piece of the file, it becomes another source of that piece to other users.

C. Digital Rights Management

With the rapid growth of the Internet, acquiring digital contents over the Internet has become commonplace. Therefore, many digital content providers sell digital contents for raising revenues. Unfortunately, situations of piracy are common and become more serious, since the digital contents can be copied and distributed easily through Internet. In recent year, Digital Rights Management (DRM) has become an emerging issue. In order to prevent the piracy to magnify, Digital Rights Management technology will be act an important role in future.

In general, there are four parties and one important framework in the DRM system architecture, that is, the content provider, the distributor, the license server, the consumer and trusted computing framework. A content provider is an entity that offers the encrypted content and establishes rules and licenses. In general, to protect the digital content, the symmetric or asymmetric cryptosystem is adopted, such as AES or RSA. The distributor is an entity that enables the encrypted content available to the consumer. A distributor enables a new distribution channel for the content provider. In general, the distributor always sets the encrypted content on its website over the Internet. The duty of the license server is to issue the license to consumer. The consumer who uses DRM system to acquire the digital content by downloading from the distributor and to purchase license for playing the content. In DRM environment, all DRM application and service are all built on the trusted computing framework. The trusted computing framework is responsible for secure distribution, execution environment, and license enforcement, supporting cryptographic functions and key management, and tamper resistance.

III. Proposed Protocol

In order to avoid copyright infringement, a well-designed protocol for preventing illegal file transmission on P2P network is necessary. P2P networks depend on the cooperation of its peers; all peers need to contribute to the file sharing process. But, there is no administrator in the system, thus, peers called *freerider* or leeching are sometime to download more data and upload few data to other peers. In P2P networks, the leeching behavior is against the nature of P2P network and violation of the health from the networks. For preventing leeching behavior, an upload-rewarding mechanism is worth to consider. Therefore, we propose a protocol which combines illegal transmission protection and reward mechanism for encouraging P2P users keep contributing. Figure 1 shows the proposed system architecture. We divided our protocol into seven phases: registration, packaging, token generation, transmission, license request, decryption and upload-rewarding phase. Table 1 shows the notations used in this paper.

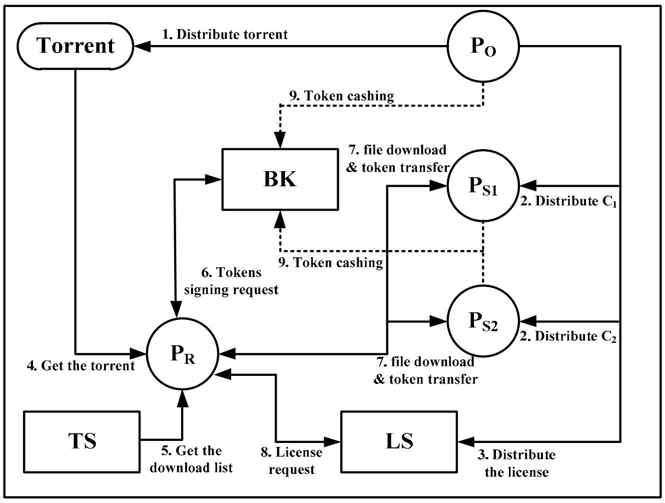

Fig. 1. System architecture

A. Registration Phase

Before join to the system, every peer is necessary to register and get the DRM module. Every peer generates its key pair, for example, peer P_i will generate the private key X_i and public key $Y_i = g^{X_i} mod\, p$. After initial process, the peer needs to setup the DRM module. The DRM module is responsible for all digital content issues including digital content decryption, license request and parse, digital content delivery etc. Furthermore, the HMAC (Hash-based Message Authentication

Code) function for peer i will embed in the DRM module and the secret key which using for calculating the HMAC is shared between peer i and BK.

TABLE I
NOTATION TABLE

Notations	Meaning
P_O	Content owner
P_R	Content requester
P_S	Content sender
BK	A trusted party (usually a bank)
TS	Tracker site
LS	License server
C	Protected content
X_i/Y_i	Private key/public key of peer i
K_e/K_d	Content encryption key/content decryption key
TK_{S_i}/TK_L	Transmission token/license token
$H_{P_i}(\cdot)$	The HMAC function for peer i.

B. *Packaging Phase*

In this phase, the content owner can generate a protected content and divide it into many small pieces. The detail process of packaging phase is illustrated as follows.

(1) P_O generates a content encryption key as

$$K_e = Y_O^a mod\ p,$$

where a is a random number.

(2) P_O encrypts the content as

$$\begin{aligned} C &= E_{K_e}(file) \\ &= file \cdot K_e\ mod\ p. \end{aligned}$$

(3) P_O divides C into C_1 and C_2. It must to note that we assume the share file is only divided into two pieces for the sake of simplicity.

(4) P_O generates and distributes a torrent file (*seed*) which includes the URL of the tracker, the BK's URL and the file information such as file name, number of bytes per piece and hash value of pieces. Everyone can download this torrent file on Internet.

(5) P_O sends the related information about constructing the license to license server (LS).

C. *Token Generation Phase*

In BT system, a peer that wants to download the file must first obtain the seed (torrent file). The torrent file includes URL of the specified tracker, which indicates the peer from which other peers to download the pieces of the file. The detail process of transfer phase is showed as follows.

(1) P_R downloads the torrent file from Internet.

(2) P_R connects to the tracker (TS) specified in the torrent file and gets a list of peers, named P_{S_1} and P_{s_2}, currently hold pieces of the file.

(3) P_R generates "number of piece of the file+1" tokens. In this case, peer P_R will generate three tokens: two transmission tokens ($TK_{S_1}$and TS_{S_2}) for the senders and one license token (TK_L) for content owner. Note that the number of piece of the file is specified in the torrent file.

(4) P_R connects to the BK specified in the torrent file and sends these tokens with his generated HMAC, $\{ TK_{S_1}, TK_{S_2}, TK_L, H_{P_R}(TK_{S_1}, TK_{S_2}, TK_L) \}$, to BK for signature. In our protocol, Schnorr-based signature [12] is used for signing tokens.

D. *Transmission Phase*

When peer P_R obtains the signed tokens, it can connect to P_{S_1} and P_{S_2} for downloading $C_1$and C_2, respectively. Peer P_R will issue a transmission token (TK_{S_i}) to the sender (P_{S_i}) after he downloaded the piece of the file (C_i). Simultaneously, the sender (P_{S_i}) will validate the signature of TK_{S_i}. The detail process of transfer phase is showed as follows.

(1) P_R connects to P_{S_1} for downloading C_1.

(2) P_R transmits $\{ TK_{S_1}, H_{P_R}(TK_{S_1}, P_{S_1}, P_R)\}$ where TK_{S_1} is a transmission token and $H_{P_R}(TK_{S_1}, P_{S_1}, P_R)$ is used to be the *evidence*.

(3) P_{S_1} transmits C_1 to P_R.

(4) Simultaneously, P_R will connect to the P_{S_2} and perform the above processes.

E. *License Request Phase*

When peer P_R completely download a file, it can connect to the license server and pay the license token (TK_L) for license request. The detail processes are as follows.

(1) LS validates the signature of TK_L.

(2) LS computes

$$\alpha_R = \left(\frac{Y_R{}^a}{Y_O{}^a}\right) mod\ p$$

$$\beta_R = g^a\ mod\ p.$$

(3) LS generates the license including α_R and β_R.

(4) LS sends the license to P_R and pays the payment to P_O.

F. *Decryption Phase*

When peer P_R receives the license, it can perform the following process to decrypt the file and enjoy it legally.

(1) P_R computes the content decryption key

$$K_d = \frac{\alpha_R}{\beta^{X_R}}\ mod\ p.$$

(2) P_R decrypts the content as

$$\begin{aligned} C \cdot K_d &= E_{K_e}(file) \cdot K_d \\ &= file \cdot K_e \cdot K_d\ mod\ p \\ &= file. \end{aligned}$$

(3) P_R updates the list of TS and letsP_R as a new *seeder*.

G. *Upload-Rewarding Phase*

This phase describes a simple upload-rewarding mechanism that using token-based mechanism and HMAC technique. When P_{S_1}obtains the token, it can connect to BK to get the payment. He needs to provide $\{TK_{S_1}, H_{P_{S_1}}(TK_{S_1}, P_{S_1})\}$ and the BK validates the above message. If the verifications are hold, BK will pay to P_{S_1}. Note that, we will discuss the dispute arbitrating process in section 4.2.

IV. RNELATED ANALYSIS

A. Fair Transaction and Encourage the Contributions

The free-riding phenomenon will reduce the performance of P2P networks. Thus, it is needs to give incentives for resource provisioning. In our proposed protocol, we allow not only the content owners can get profits, but also the content senders will get rewards from their upload contributions. If the senders keep uploading many files, they can get more payment.

B. Check for Double Spending

A dispute arises when a content requester double spending a token or a content sender share a token to other peers. In the first condition, a malicious peer P_m has received a token that signed by BK and transmits the token to P_{S_1} and P_{S_2}. If P_{S_1} first submits the token to cash it in BK, he will successfully cash the token, and the token will be marked spent. Hereafter, P_{S_2} submits the token to cash it also, and BK will find this token is double spent. Thus, BK will ask both P_{S_1} and P_{S_2} to submit the *evidence* for arbitrating the dispute. When BK receives the *evidence* $(H_{P_m}(TK_{S_1}, P_{S_1}, P_m))$ from P_{S_1} and P_{S_2}, he can find out the token is issued by P_m. In the second condition, a content sender P_{S_1} that holds a valid token (TK_{S_1}) obtained from P_m and he sends the token to P_{S_2} for cheating. Obviously, it is cannot work in our protocol. When a token submitted to the BK twice for cashing, the BK will find the token is double spent. Thus, BK will ask both P_{S_1} and P_{S_2} to submit the evidence for arbitrating the dispute. Because the token that submitted from P_{S_2} is not obtained from P_m. Thus, P_{S_2} cannot provide the correct *evidence* $(H_{P_m}(TK_{S_1}, P_{S_2}, P_m))$. Note that, if P_{S_2} provides the correct *evidence*, it means that P_m is cheating by double spending.

C. Non-repudiation

Non-repudiation is a most important requirement in a transaction system. In our protocol, we employ the Schnorr-based signature and HMAC technique to achieving the property of non-repudiation. In token generation phase, content requester needs to send the generated tokens with his generated HMAC to BK for signature. The BK will use Schnorr-based signature to sign these tokens and send back to content requester. A digital signature is generated using the private key of a key pair and is commonly used for offering the property non-repudiation.

In general, HMACs do not provide the property of non-repudiation. Since any user who can verify a HMAC is also capable of generating HMACs. However, in our protocol, the BS is a verification party and it is a trusted third party. Thus, we use HMAC technique to meet the requirement for computational cost consideration. In upload-rewarding phase, content sender P_{S_i} sends $\{TK_{S_i}, H_{P_{S_i}}(TK_{S_i}, P_{S_i})\}$ to BK, the value of $H_{P_{S_i}}(TK_{S_i}, P_{S_i})$ can only be generated by P_{S_i} and BK where BK is a trusted party. Thus, we convince that only P_{S_i} can generate the $H_{P_{S_i}}(TK_{S_i}, P_{S_i})$.

V. CONCLUSIONS

In this paper, we propose a DRM mechanism for BitTorrent-like P2P Systems. We employ token-based payment mechanism and HMAC technique. The HMAC is used for constructing the evidence which can arbitrate the disputes. We also designed a transaction mechanism that protects more content owners' profit but also the rewards for content senders. In our protocol, we provide upload-rewarding for senders. It will encourage users to keep sharing their own files that can solve the free-riding phenomenon and improve the performance of P2P networks.

ACKNOWLEDGMENT

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract NO: NSC 99-2221-E-005-094.

REFERENCES

[1] C.T. Yen, H.T. Liaw, N. W. Lo, T. C. Liu, and J. Stu, "Transparent Digital Rights Management System with Superdistribution," in Broadband, Wireless Computing, Communication and Applications, 4-6 Nov. 2010.

[2] C. C. Yang, J. C. Hsiao, H. W. Yang, and J. Y. Jiang, "Convertible DRM System Based on Identity-Based Encryption," International Journal of Computer Networks & Communications, 2009, 1(3).

[3] N. Y. Lee and T. Y. Lee, "User Friendly Digital Rights Management System Based on Smart Cards," in International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 12-14 Sept. 2009.

[4] C. C. Yang, J. Y. Jiang, and J.C. Hsiao, "Trusted DRM on P2P network," Journal of Computers, 2009, 20(3).

[5] Y. Y. Chen, J. K. Jan, Y. Y. Chi, and M.L. Tsai, "A Feasible DRM Mechanism for BT-Like P2P System," in International Symposium on Information Engineering and Electronic Commerce, 2009, Ternopil, Ukraine.

[6] W. Diffie and M. Hellman, "New directions in cryptography," Information Theory, IEEE Transactions on, 1976, 22(6): p. 644-654.

[7] Zhang Xinwen, Liu Dongyu, Chen Songqing, Zhang Zhao, and S. Ravi, "Toward digital rights protection in BitTorrent-like P2P systems," in The 15th SPIE/ACM Multimedia Computing and Networking, 2008.

[8] C. C. Yang, Y. R. Lin, and J.C. Hsiao, "Authorized file-sharing system on P2P networks," in Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, 2010, Caen, France: ACM

[9] J. S. Beuscart, "Napster Users between Community and Clientele: The Formation and Regulation of a Sociotechnical Group," Sociologie du Travail, 2005, 47: p. e1-e6.

[10] I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications," ACM Transactions On Networking, 2003, 11(1): p. 17-32.

[11] A. Rowstron and P. Druschel, "Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems," in In Proc. IFIP/ACM Middleware, 2001.

[12] C. P. Schnorr, "Efficient signature generation by smart cards," Journal of Cryptology, 1991, 4(5): p. 161-174.