The Journal of Systems and Software 83 (2010) 1689–1700

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

A novel DRM framework for peer-to-peer music content delivery

Jung-Shian Li*, Che-Jen Hsieh, Cheng-Fu Hung

Department of Electrical Engineering, Institute of Computer and Communication Engineering, National Cheng Kung University, 1, University Road, Tainan, Taiwan

ARTICLE INFO

Article history:
Received 20 September 2009
Received in revised form 4 April 2010
Accepted 4 April 2010
Available online 15 June 2010

Keywords:
DRM
RSA
P2P
Fingerprint
Data hiding
Content delivery

ABSTRACT

Due to rapid advances in the network communications field in recent years, the distribution of large-scale music contents has become easier and more efficient than ever before. However, the unauthorized distribution of copyright-protected content has emerged as a major concern. Accordingly, this paper presents a content distribution framework with a DRM capability for P2P networks. The robustness of the content distribution is ensured by using a network coding approach based on the Lagrange polynomial interpolation method. When the downloading peer within the network receives sufficient coded pieces, it not only reconstructs the associated blocks using a finite field Gaussian elimination method, but also creates its own copies of the coded pieces within these blocks and shares these copies amongst the other peers in the network. As a result, the distribution overhead imposed on the music provider is substantially reduced and the number of coded pieces within the network is significantly increased, thereby overcoming the “last piece problem” inherent in existing P2P schemes. In the DRM module of the framework, the RSA public-key cryptosystem is used to generate a unique digital fingerprint for every user within the network. The fingerprint is embedded within the music file in a protected form such that the music provider can establish the identification of any user performing an unauthorized distribution of the file. The experimental results confirm that the proposed framework provides an efficient and secure means of distributing large-scale copyright-protected music contents with no discernible degradation in the audio quality.

1. Introduction

Recent developments in the network communications field now make possible the efficient distribution of digital contents by both experts and novices alike. However, the ability to make perfect copies and the ease with which these copies can then be distributed have given rise to significant problems regarding the misuse, illegal copying and distribution, plagiarism, and misappropriation of copyright-protected content (Lee et al., 2002; Eugene and Reginald, 2005).

Although it is common practice to deliver multimedia contents over the Internet nowadays, the problem of data security is emerging as a major concern. Therefore, multimedia contents are generally encrypted in some way to prevent unauthorized users from accessing the data (Grangetto et al., 2006; Wu and Kuo, 2005). However, while such techniques can protect the multimedia contents during their transmission, they cannot prevent a user from distributing the data illegally once they have been received and decrypted. It has been suggested that this problem can be resolved to a certain extent by embedding a watermark of some kind in the transmitted contents in order to establish a digital rights management (DRM) capability (Li et al., 2007; Lan et al., 2009; Macq et al., 2004; Lei and Soon, 2009; Wang et al., 2002). In addition, a technology referred to as digital fingerprinting has been proposed as a means of identifying users illegally distributing copyright-protected material by inserting a unique identifier ID into each user's copy of the file (Wagner, 1983). Both techniques have a proven ability to protect multimedia contents from unauthorized tampering and distribution, and have therefore attracted considerable attention in the literature (Wu et al., 2004; Burges et al., 2003; Luh and Kundur, 2005; Kundur and Karthik, 2004; Zhu, 2009).

This study presents a novel framework for the delivery of large-scale music contents over peer-to-peer (P2P) networks. The proposed scheme is compatible with any existing P2P network and not only ensures the integrity of the delivered data, but also provides a DRM capability. A robust content distribution is obtained by performing network coding using a Lagrange polynomial interpolation technique. The simulation results demonstrate that the proposed framework yields an effective reduction in the overhead and avoids the last piece missing problem in the network.

In a centralized multimedia providing service, each client downloads the requested data from the server directly, and thus scalability problems may arise. While P2P distribution systems such as Napster (Napster, 2000) and Gnutella (Ripeanu and Foster,

* Corresponding author.
E-mail address: jsli@mail.ncku.edu.tw (J.-S. Li).

0164-1212/$ – see front matter. Crown Copyright © 2010 Published by Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2010.04.071

2002) are scalable, they are ill-equipped to deal with the copyright protection problem. Accordingly, the present study develops a novel framework for the delivery of large-scale music contents over P2P networks which not only resolves the scalability problem, but also provides a DRM capability by embedding digital fingerprints in each user's copy of the file at the egress node when the pieces of the transmitted file are assembled to reconstruct the original music file.

In the proposed framework, the music file is partitioned into network-coded pieces by the music provider (MP) and is then distributed over the P2P network. When a user has received sufficient coded pieces, he or she can retrieve the original music file. A servlet installed on the user machine combines the received coded pieces and unique user identification into a DRM-enabled music file using a novel data hiding mechanism and the RSA public-key cryptosystem (Rivest et al., 1978). The "servlet" is a kind of Java technology to extend and enhance service. Servlets provide a component-based, platform-independent method for building applications in multi-tiered systems. Significantly, the proposed network coding mechanism extends the time for which the data is available within the P2P network. In general P2P networks, individual peers may leave the network as soon as they have received all of the pieces of the music file. Since peers may leave the network after they have received all pieces, it is possible for some pieces to become rare. As a result, a peer cannot receive the music file if any piece disappears. It is so-called the last piece missing problem. In the proposed framework, this problem is resolved using a network coding scheme based on the Lagrange polynomial interpolation technique. Furthermore, the distributed digital fingerprint scheme is performed in an efficient way and prevents unauthorized users from distributing the music file.

This paper is motivated from three components, P2P networking, network coding and digital right management (DRM) to build a system. The proposed network coding mechanism is enhanced from the linear combination to combat the last piece problem and reduces lots of overheads. The fingerprint embedding mechanism is simple and robust compared to the existing ones. Furthermore, a prototype is built in our network security testbed and the experimental results show that the framework is workable.

The major contributions of the P2P DRM framework presented can be summarized as follows:

(1) The framework motivated from P2P networking, network coding and DRM builds a secure, scalable and robust system for dissemination of music content over the Internet. It is fully compatible with all existing P2P schemes.
(2) The original music file is partitioned by the MP and coded using the Lagrange polynomial interpolation method. Once the downloading peer has received sufficient coded pieces, it reconstructs the corresponding pieces using a finite field Gaussian elimination method (Helton and Helton, 2002) and creates copies of the coded pieces within these blocks using its own ID. It then shares these pieces with the other peers in the network. This not only reduces the distribution overhead imposed on the MP, but also increases the number of coded pieces within the P2P network and therefore resolves the "last piece problem" inherent in conventional P2P schemes in which some of the peers need to wait for a long time to receive the final piece of the music file.
(3) The RSA public-key cryptosystem is used to generate a unique digital fingerprint for each user, and thus the MP can readily identify any misbehaving users making unauthorized distributions of the music file.
(4) The digital fingerprint is hidden in the music file using a commercial steganography tool such that its presence is not obvious to a causal observer. Moreover, the robustness of the fingerprint toward deliberate attack by a malicious user is improved via the use of an error-correcting code polling technique.
(5) The study has built a prototype in our network security testbed. The experiments show the idea workable in practice. The framework can be easily extended to other types of multimedia files, such as JPEG or MPEG, by integrating the corresponding fingerprint schemes (Luh and Kundur, 2005; Kuribayashi and Tanaka, 2005).

The remainder of this paper is organized as follows. Section 2 presents a brief overview of the related studies within the literature, while Section 3 provides the preliminaries for the proposed framework. Section 4 discusses the details of the P2P DRM scheme. Section 5 discusses the implementation and extensibility issues and analyzes the computational complexity of the proposed framework. Section 6 presents the results of a series of experiments designed to evaluate the performance of the DRM framework. Finally, Section 7 presents some brief concluding remarks.

2. Related work

To provide DRM in P2P networks, the content distribution methodology should be discussed at first. Each peer is the client as well as the server and the content dissemination is performed in a fully distributed manner. So, it is difficult to identify the source of the content distributor. Consequently, digital rights management is an important means to stop the illegal content circulation by examining the potential unlawful distributor and identifying the source of the piracy. Data hiding in the content, the so-called digital fingerprints, is the key technique for the success of P2P DRM schemes.

2.1. Content distribution

Network content dissemination is a simple way for the distribution of digital content. The need for this service is due to the increasing number of users in the network. Consequently, it is important for achieving a high availability in content delivery. While many overlay networks have been proposed for realizing content delivery services, Content Delivery Networks (CDN) (Peng, 2003; Vakali and Pallis, 2003) and P2P networks are amongst the most commonly applied.

CDN was first developed as a means of replicating content over several servers placed inside or at the edge of the Internet (Douglis and Kaashoek, 2001). One of the best examples of the CDN approach is that of Akamai (2008), which operates several tens of thousands of servers all over the world. In theory, CDN should provide resilience to "flash crowds" (Arlitt and Jin, 2000). However, in practice, a huge and sudden surge of traffic generally causes the server to collapse. Furthermore, CDN suffers a scalability problem in that the system efficiency is severely degraded when large numbers of users access the network simultaneously. Therefore, P2P network solutions have gained in popularity in recent decades as a means of delivering content efficiently to a large number of Internet users without routing the content through servers. However, existing P2P systems such as BitTorrent (Cohen, 2003) suffer a number of drawbacks, including a high churn rate and a missing last piece problem. In the current study, these problems are resolved by developing a novel P2P framework implemented using a network coding scheme based on the Lagrange polynomial interpolation technique.

2.2. DRM

With the proliferation of Internet-based applications and the ready availability of powerful file sharing and distribution tools, DRM has become a critical concern in the Internet domain. Two