RC 21917 (98565) 22 December 2000 **Computer Science**

IBM Research Report

Scalable Distribution of Copyrighted Content Using Digital Video Broadcast Networks

Magda Mourad, Jonathan Munson, Giovanni Pacifici, Ahmed Tantawy, Alaa Youssef

IBM Research Division
Thomas J. Watson Research Center
P.O. Box 703
Yorktown Heights, NY 10598

Scalable Distribution of Copyrighted Content Using Digital Video Broadcast Networks

Magda Mourad, Jonathan Munson, Giovanni Pacifici, Ahmed Tantawy and Alaa Youssef

IBM T.J. Watson Research Center

P.O. Box 704

Yorktown Heights, NY 10598

USA

{magdam, jpmunson, giovanni, ahmed1, ayoussef}@us.ibm.com

Abstract

Building on recent advances in digital rights management, digital video broadcast networks, and interactive TV, we present a system that lies at the intersection of these evolving technologies. The system presented in this paper combines the powers of these technologies, in a novel way, and represents a new generation of scalable, far-reaching, secure e-commerce systems for trade in copyright protected content.

The introduced system enables users, tuning to a digital TV channel, to be presented with entertainment material that promotes digital content available for download over the same broadcast channel (e.g., a music video that promotes an audio album available for download). Users, interacting with an application running on the set-top box, can either select and download the promoted content to a secured end-user device, or browse a catalog of all digital content offered for download. The MPEG-2 standard transport stream for broadcast transmission is a natural candidate for the communication

channels used in the system, as it allows the solution to be deployed over virtually all types of digital broadcast networks.

Key words: copyright protection, digital video broadcast, e-commerce.

1. Introduction

The use of global distribution systems, such as the Internet, for distribution of digital assets, such as music, films, computer programs, games, courseware material, and other content continues to grow. At the same time owners and publishers of valuable digital content have been slow to embrace the use of the Internet for distribution of digital assets for several reasons. The first and foremost reason is that the owners are afraid of unauthorized copying or pirating of digital content. One barrier that is removed with electronic distribution is the requirement of the tangible recordable medium itself (e.g., diskette or CD). However, copies of electronically distributed digital content are identical to the original. For example, a printed picture, when reproduced by photocopying, the copy is of lesser quality than the original. Each subsequent copy, sometimes called a generation, is of less quality than its predecessor. This degeneration in quality is not present when a picture is stored digitally. Each copy and every generation of copies is as clear and crisp as the original.

The aggregate effect of perfect digital copies combined with the very low cost to widely distribute content electronically makes it relatively easy to pirate and distribute unauthorized copies. Therefore a need exists to ensure the protection and security of digital assets distributed electronically. Recent advances in the area of digital rights management (DRM) provide evolving solutions to this problem [EMMS, CG, Intertrust]. In this regard, we show how our system leverages on the capabilities of IBM's Electronic Media Management System (EMMS) [EMMS] to achieve copyright protection for downloadable content.

Another reason digital content providers have been slow to adopt electronic distribution of digital content is the time latency it takes to download content to the end user, and the inefficient utilization of bandwidth inherent to the traditional Internet model of unicast distribution. A compressed music album, which maintains a high quality audio grade, may reach over 100 megabytes in size. Using a 56 kbps modem, downloading this album takes well over 4 hours, especially when accounting for message headers and retransmission overheads. File sizes for high quality video content are much more problematic. Even rich multimedia courseware presentations may reach a few megabytes in size. Delivering digital content over broadband infrastructures, such as satellite and cable TV networks, provides an attractive solution to the problem of latency. Additionally, these broadband infrastructures typically deploy transport protocols, such as the MPEG-2 transport stream [MPEG], with basic built-in support for broadcast, which can solve the problem of efficiently utilizing the available bandwidth for content distribution.

Still another reason digital content providers have been slow to embrace electronic distribution of digital content is their desire to maintain and foster existing channels of distribution. The use of electronic distribution can remove the ability of retail stores to differentiate themselves from each other, especially on the Web. Therefore a need exists to provide retailers of electronic content with a way to differentiate themselves from each other, especially by means of offering new distribution channels, that can reach more and more of their consumers. The use of interactive TV, combined with data broadcast channels, for promotion, distribution and fulfillment of e-commerce transactions in digital content seems appropriate for this purpose.

In this paper, we describe how we combine advances in digital rights management, digital video broadcast, and interactive TV, to build a system that provides end-users with new convenient easy-to-use shopping experience, the content owners with additional secure channels for reaching more consumers, and the distributors with new e-commerce revenue streams and distinguishing distribution channels.

The rest of this paper is organized as follows. In Section 2, a brief survey of background and work in the relevant areas is presented. Section 3, illustrates the overall end-to-end architecture. In Section 4, we take a closer look at the design details and implementation issues. Section 5 discusses the pros and cons of the system and brings attention to some of the important issues that arise in secure distribution of copyrighted content. Finally, we present our concluding remarks in Section 6.

2. Background and Related Work

In this section, we briefly describe each of the fundamental technologies, which the presented system is built on.

2.1. DRM Systems

The unprecedented growth of the Internet has made it forceful and persuasive for producers to distribute content to a worldwide audience faster and more efficiently than ever before. While all types of digital content publishers have invested heavily in building their Internet presence, most of them find that they are spending on their Web sites several times more than they are earning from advertising and other revenues. In many cases, digital content publishers find their traditional sources of revenue being eroded by the ability of consumers to obtain information freely and illegally from a publisher's Web site or from newsletters, research reports and similar content delivered via electronic means such as e-mail.

With conventional technology, regardless of how sophisticated a subscriber and access control systems are, once digital content has left the Web server for a consumer to view it or play it, the publisher looses the ability to monitor and control the usage of the copyrighted content. Re-use and redistribution are a simple task threatening the very core of publishing as a business. For all its challenges, the Internet represents a vast new marketplace for publishers, as long as they can control the distribution and use of their valuable content through a flexible and minimally intrusive DRM system.

Several researchers have recently focused on DRM issues [Lowt00, Brass99, Choud95, Kohl98]. Also, several DRM systems have appeared on the market in the past few years. In general, all DRM systems allow the distribution of digital contents in an encrypted form. A set of rights is associated with each single piece of content, and only after acquiring the rights of accessing a protected piece of digital content will a user be allowed to decrypt it. In robust DRM systems, users are typically prevented from directly decrypting the content, saving it, and distributing it in a decrypted form, These controls are usually exercised within special software modules running in the consumer's devices. These protected (i.e., trusted or tamper resistant) player/viewer modules are therefore needed for the users to access the content and use it in a manner compatible with the rights they purchased. Examples for such systems include IBM's EMMS [EMMS], ContentGuard originally from Xerox [CG], and the Metatrust system from Intertrust [Intertrust].

Therefore, users must install special players in order to access any protected content that is downloaded to their machines. This approach may be secure enough to protect copyrighted material, but does not lack inflexibility. In fact, the main problems associated with this approach are the dependency on a specific trusted player, and the limited content types that can be accessed by that player. In order to avoid such drawbacks of existing DRM systems, and to achieve the desired flexibility and minimal intrusion in the DRM system design, we introduced a novel approach to supporting DRM requirements on the client side, which is completely transparent to the player application [Mour01]. This means that the DRM system does not interfere with the player development phase at all. In fact, the player developers need not be aware that their application will be used to render protected content. Additionally, transparent DRM extensions can be added to any extendible content viewer/player, hence eliminating dependency on a particular viewer application or content type. Further discussion of this approach, however, is beyond the scope of this paper.

2.2. Generic DRM System Architecture

Figure 1 depicts the components of a typical DRM system. There are five basic components necessary for creating a complete end-to-end DRM-enabled e-commerce platform. These are described briefly below.

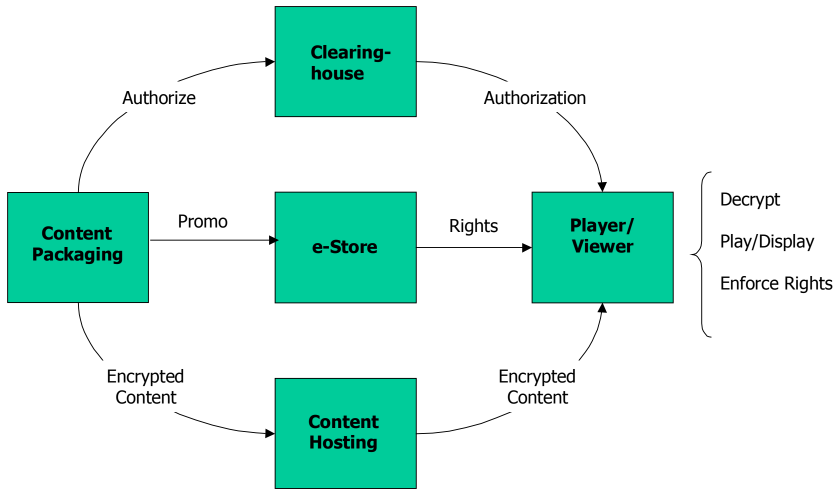

Figure 1: Generic DRM system architecture.

- ***Secure Content Packaging.*** This component is responsible for content encryption and packaging, on the publishing side. Content packaging is the last step in the authoring phase, and ideally the packaging tool should be seamlessly integrated with the authoring tool. The packaging tool could be Web-based with an easy to use user interface that could be manually operated, to specify the content files and rights. Alternatively, the interface between the packaging and authoring tools could be an automated one.
- ***E-Store.*** The e-store represents the only tangible interface between the end-user and the entire system. The e-store is responsible for advertising the content, for accepting payments and most importantly for generating authorization tokens (certificates) that include the purchased rights.
- ***Content Hosting.*** This component is responsible for hosting the encrypted content packages and releasing them only to authorized users, who have acquired the rights to

download the content. Logically separating this component from the rest of the system allows for flexibility and independence of the distribution channel used.

- ***Clearinghouse.*** This component is responsible for personalizing the keys for decrypting the content for each individual user. It is also the focus of authorization and usage tracking. In general, the Clearinghouse is the only component that is trusted by all parties (content owners/publishers, distributors, and consumers).
- ***Player/Viewer.*** This component runs on the client side and encapsulates the DRM client. The DRM client is responsible for accessing the content, interacting with the Clearinghouse, maintaining the content encrypted using keys that are hidden from the user at all times, and enforcing the usage conditions associated with the content. Traditionally, the DRM client has been always embedded inside a customized player/viewer, and the two modules together form one trusted application that is installed on the client machine. The protected content cannot be rendered using any other player/viewer.

2.3. Digital Video Broadcast Networks

Recent advances in telecommunications led to the migration of most of today's cable and satellite broadcast networks to the digital world. Probably, the most profound factor that facilitated this migration was the MPEG-2 standard [MPEG], which defines how elementary audio, video, and data streams are combined into one composite stream that maintains their temporal relationships and is suitable for storage or transmission. First, a basic multiplexing approach adds, to each stream, system-level information, and each stream is packetized to produce a *Packetized Elementary Stream (PES)*. Subsequently, the PESs are combined to form a P*rogram* or *Transport Stream*. The program stream is similar to the Mpeg-1 stream and is aimed at a relatively error-free environment. The transport stream, on the other hand, is well-suited for transmission of digital television and accompanying data streams (normally used for interactivity and other applications) over fiber, satellite, cable, ISDN, ATM, and other networks [Stei95]. The transport stream is designed for use in lossy or noisy media. It combines the PESs and one or more independent time bases into a single stream with 188 bytes long packets, including a 4 bytes header.

Several systems exist to provide information over broadcast infrastructures. Some of them encapsulate IP packets within MPEG-2 streams, and others use other packetization schemes, typically over MPEG-2 as well. These systems are not integrated with a secure digital rights management system. The lack of security makes the digital content delivered over these systems easy to pirate. Moreover, many of these systems require a back channel, usually a phone line, to select the digital content desired. If the back channel is not available, the content cannot be selected. Other systems do not provide promotion data, content data, and metadata in a single digital channel, but require an additional bi-directional channel for one or more of these functions. Accordingly a need exists to overcome these obstacles.

Our system may optionally use a bi-directional channel, if it is available, mainly for efficient retransmission of corrupted data blocks as well as for download-on-demand, if desired by the distributor. For the latter case, the literature is rich with algorithms for scheduling transmission, for dissemination-oriented applications in which a large client population requests data items from an information source equipped with a data broadcasting capability [Aksoy99].

Consumers can become more involved with TV shows through interactive television programming. Viewers can play along with leading game shows, find out more information during favorite shows, or buy the merchandise they see advertised through a click of a button on the remote control. Some statistics indicate that, in the United States alone, more than 700 hours of weekly programming are now interactive. Our aim is to coordinate this interactivity with simultaneous data broadcast channels, in a way that creates the ability to select and instantaneously download digital content from the broadcast stream, while watching TV.

3. Architecture Overview

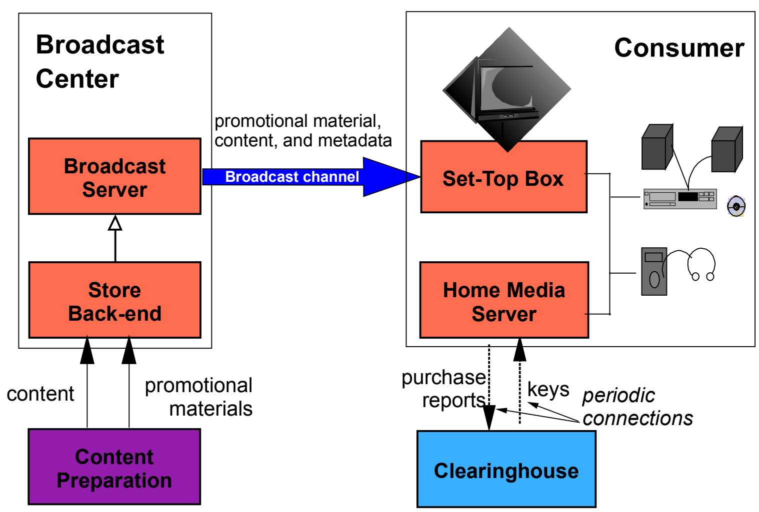

Figure 2: Broadcast-based DRM system architecture.

Figure 2 represents the architecture of a broadcast-based DRM system. At a first glance, this diagram looks similar to the one presented in Figure 1. However, careful inspection of the diagram reveals several subtle differences. Aside from using a broadcast channel to reach multiple clients simultaneously, a significant difference appears in combining the content hosting and e-store functions together. In essence, the broadcast server, in this model, is responsible for generating and broadcasting the e-store front, which presents promotional material to the user, mostly in the form of video clips in this case, in addition to broadcasting the content. Therefore, the information flowing on the broadcast channel must be self-contained: content, promotional material, as well as catalog and addressing information for downloading different content selections.

Another difference appears on the consumer side, where a receiver device, such as a set-top box, is necessary to receive, interpret, and filter the broadcast stream. The receiver device may be connected to a home media server, or simply a PC, where the content is ultimately ingested and securely stored encrypted at all times. The content may be checked out, temporarily, to hand-held devices, which implement a secure interface such as that recommended by the Secure Digital Music Initiative [SDMI][reference?].

Still another difference between a traditional DRM system and a broadcast-based one appears in the nature of the connection to the Clearinghouse (CLRH). In the broadcast model, it may not be desired to establish a back-channel connection to the CLRH after each download, to get the authorization for using the new content. This flexibility comes at a cost of added complexity to the system, which we address later in Section 5.

4. System Design and Prototype Implementation

A prototype based on the illustrated high-level architecture was implemented. Details of the system design are described below.

4.1. Content Packages

The digital content is organized into *packages*. Each package is associated with *promotional material*, *meta-data*, *package descriptor, and* an optional *video-clip*. The promotional material consists of graphics and text material associated with the package content (e.g., cover art associated with a music album); the meta-data is a set of attribute-value pairs (e.g., title, price, artist, etc.); a package descriptor is a set of attribute-value pairs that are used for extracting the structured digital content from a package (e.g., package-size, number-of-sections, etc.); the video-clip presents and promotes the content of the package (e.g., a short music video promoting a music album). The video-clip is in fact promotional material, however, we distinguish it from the rest of the promotional material since its sole purpose is to be displayed on TV, as part of normal broadcast programming.

A broadcast server in one or more digital broadcast channels in a carousel fashion transmits the packages, as well as the promotional material, video-clips, meta-data, and package descriptors. A carousel is a continuous digital stream that repeats itself over a set of *broadcast intervals.* A broadcast receiver allows a user to select and download packages as well as extract the digital content from a package.

Packages are organized in two sets: *static offering* and *dynamic offering*. The *static offering* represents the set of *active* packages, i.e., packages that are currently being broadcast in a carousel fashion. The dynamic offering represents a set of packages that are available at the server and are not currently being broadcast. The static offering set is in turn organized in two subsets: a set of packages that have active video clips, and a set of packages that do not have active video clips, but are listed in a catalog.

4.2. User Interaction Model

An application running on the *broadcast receiver* (BR), which is typically a set-top box, provides a video decoder, a graphical user interface and receives user input. The set-top box allows the user to tune to a digital TV channel to display video clips associated with some of the static offering packages. The set-top box allows the user to select packages for download from both the static offering and dynamic offering sets. Users select and download static offering packages by selecting an appropriate icon, which is super-imposed by an application running on the set-top box, over the video clip associated with a package. Alternatively, users may select and download static offering packages by navigating a catalog using the remote control.

Selection, download, and extraction of static offering packages does not require a back channel for the exchange of additional information between the broadcast sender and receiver.

Users select and download dynamic offering packages by navigating another catalog to locate the desired selection. The set-top box communicates with the broadcast server, using a back channel, to request the broadcast of this dynamic offering package. The broadcast server, collects all requests from the users set-top boxes and implements a scheduling algorithm that assigns packages to carousels and carousels to broadcast intervals. Once a dynamic offering package is assigned to a carousel (and therefore to a broadcast interval) it becomes a static offering package.

4.3. Master and Active Catalogs

All the packages' *promotional material*, *meta-data and descriptors* are collected inside a *master catalog*. The master catalog is broadcasted constantly in a pre-set carousel at a very low rate. The packages belonging to the static offering set are listed in an *active catalog*. The active catalog contains the following:

- broadcast addressing information necessary to receive static offering packages;
- broadcast addressing information to receive the video clips;
- broadcast addressing information necessary to receive the master catalog;
- an identifier for the package whose video clip is currently being broadcast;
- a set of identifiers for the packages belonging to the static offering set;
- master catalog version;
- active catalog version.

Since the active catalog contains only identifiers and simple addressing information, it is very compact and can be updated frequently. In this fashion the BR can be always up to date with the state of the broadcast channel.

4.4. Reliable Transmission

To build and represent the graphical user interface the set-top box downloads the master catalog and extracts the contained data. To download a selected package the set-top box tunes to the carousel that contains the package and then starts collecting the data associated with the package. Package data is organized in sections. Due to digital transmission errors, sections maybe corrupted and/or lost. Sections integrity is determined using CRC-32 style information. Typically, the set-top box will gather all the package sections over carousel cycles. After all sections have been collected and re-ordered the set-top box can re-assembles the package. If a separate bi-directional unicast channel is available, the set-top box can use this channel to collect the missing package portion. Using the latter mechanism the package download time is reduced significantly.

4.5. E-Store Management

A store manager application is used to build the *static offering* and the *dynamic offering* sets. The same application is used also to associate packages to carousels and determine the broadcast intervals of each carousel and each video clip. The actions performed by the broadcast manager application are communicated in real-time to the broadcast server, which acts upon them instantly.

The package descriptors and the promotional material are broadcasted using a two-phase paradigm that allows for the real-time update of the receiver.

4.6. End-to-end Content Broadcast Distribution

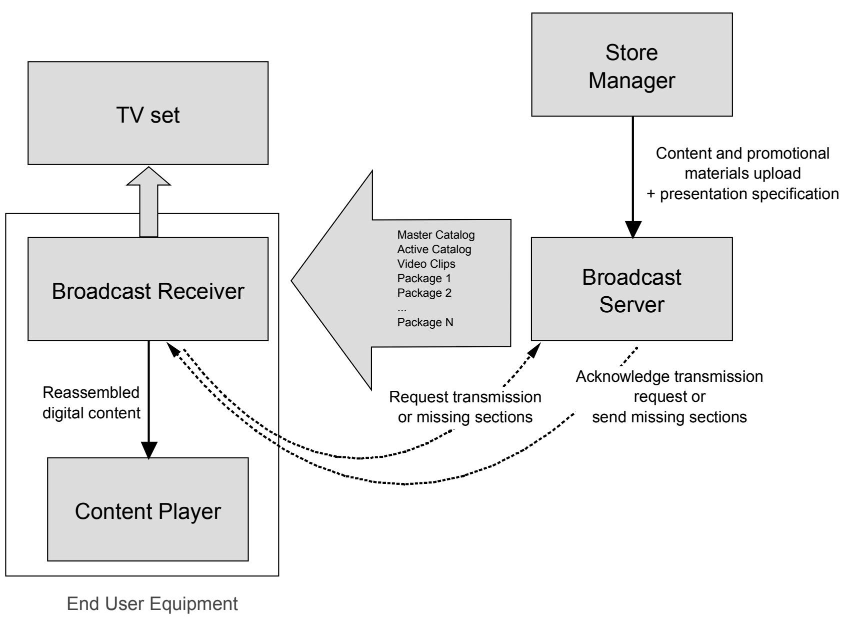

Figure 3: End-to-end content broadcast system.

The main components of the content distribution system are illustrated in Figure 3. The system is composed of a Store Manager (SM), a Broadcast Sserver (BS), and a Broadcast Receiver (BR) application and Content Player application (CP). The task of the SM is to build the *static offering*, and the *dynamic offering* sets, and associate packages to carousels and determine the broadcast intervals of each carousel and each video clip. The BS is responsible for broadcasting the master catalog, the active catalog, the active carousels and the video clips. The BR collects the catalog information, displays the video clips on the user TV set and runs the application that allows users to select and download packages. The BR extracts and collects the sections associated with a desired package and re-assembles the package. The CP allows user to store and play the digital content (again, the term "play" is used broadly). The CP is usually executed on a home digital terminal, such as a set-top box or a PC with the necessary broadcast terminal electronics. The BR is a single logical module; it may be realized in separate software modules, which may or may not execute on separate physical devices.

Based on the information carried in the active catalog, the BR partially overlays the video clips with icons representing the actions the user may take at every instant in time. The two main actions which the user may take are to request to download the currently advertised content, or to browse the static offering or dynamic offering catalog. The BR overlays the viewing material with the correct icons of only permissible user actions. After the user selects the content to download, the BR may, if necessary, contact a server to perform typical user authentication/credit authorization steps. If the selected package belongs to the dynamic offering set, the BR contacts the BS (if such a channel is available) and requests the broadcast of the selected package. After receiving the BR request the BS validates the request and schedules the transmission of the desired package. The BS replies to the BR with an acknowledgement of the broadcast as well as the broadcast intervals associated with the carousel carrying the selected package. The BR may displays the broadcast intervals to the user and requests the selection of a specific interval.

At download time, the BR tunes to the digital channel specified in active catalog, and begins filtering the desired package sections out of the multiplexed broadcast stream. The BR detects transmission errors and suppresses corrupted blocks (the mechanism used in our prototype is cyclic redundancy check). The BR reassembles the package using the package descriptor information contained in the master catalog. After the successful download of a package in the dynamic offering set, the BR notifies the BS.

The system also has the ability to use a separate unicast network connection between the BS and the BR to expedite the recovery of corrupted sections. Since the number of corrupted sections is typically low, the volume of retransmitted data is low and hence it is faster to retransmit these sections over the a unicast network connection using unicast or multicast, as opposed to waiting for a full carousel cycle. Furthermore, if the BR determines that it would be faster to download the entire package over this channel, it may also do so.

5. Discussion

While several researchers have focused on studying Internet-based e-commerce systems for content distribution, less attention was given to systems utilizing broadcast networks for distributing protected digital content. In this section, we address some of the issues and problems, which are unique to this environment, and present our approach to tackling them. It should be noted though that the solutions presented here could be adapted to other distribution environments, e.g., using wireless communications.

5.1. Key Management in Disconnected Operations

In Section 3, it was mentioned that in some broadcast setups, it might be desired to connect only periodically to the CLRH, not after each download, for authorization. In order to achieve this flexibility, a global key is used. The global key virtually corresponds to a CLRH's pre-authorization to all downloads. While this key is kept secretly by the DRM, it creates a vulnerability to potential hacker attacks. In order to minimize the potential damage caused by an attack, or stated alternatively, in order to increase the relative cost of an attack to the potential benefit gained from breaking a key, the global key expires after a period of time, T, where the shorter T is, the higher is the relative cost of the attack. At the end of each T interval, the client must connect to the CLRH to get the new key. In doing so, the DRM client reports all the transactions that took place since the previous connection. Also, within T, another constraint exists, which is a certain quota, Q, specified in monetary value or number of packages the user is not allowed to exceed within any T interval, unless a connection is made to the CLRH. Thus, T and Q together constraint the potential benefit behind an attack on the global key.

The global key is, in fact, used to encrypt the symmetric keys, which in turn are used to encrypt the content. Thus, every T interval, an overhead of re-encrypting the symmetric keys of all content packages is introduced.

5.2. Combining Broadcast Distribution and Web-based Promotion

In our discussion so far, we have always assumed that the broadcast medium multiplexes content packages together with promotional material and meta-data. However, there could be situations where this aggregation of promotion and content download channels over the same broadcast medium is not desired. For example, a distributor may desire to promote content, and perform e-commerce transactions on a Web site, while taking advantage of the efficiency of the broadcast model in downloading the content to the user's set-top box or PC.

This seemingly simple scenario entails additional requirements to the system. First, the Web-based promotion server needs to be tightly coupled with the broadcast server transmitting the content, in order to provide clients with current offerings that are actually being simultaneously broadcast. This is particularly important for static offerings. In case of dynamic offerings, tight coupling between the two servers is needed to return to the client accurate download time schedules and package addressing information, for correct de-multiplexing of packages off the broadcast stream. This coupling may take a many-to-one shape, if multiple local broadcast stations, serve content promoted by a single national Web site.

Second, if the Web browser and broadcast receiver do not both run on the same device or host, communication between the two devices is required, by using a LAN, or some other sort of direct connection. This happens, for instance, when a user uses his PC to run the Web browser, while the broadcast input feeds only his set-top box. In this case an application must be always running on the set-top box and ready to receive connections initiated by the PC, which places a stringent requirement on the set-top box capabilities.

6. Conclusion

Scalable secure distribution of copyright protected digital content poses several challenging problems that have kept such systems lagging behind in utilizing their full potential. First, the large sizes of content packages represent a challenge in their transmission within reasonable latency, and with efficient utilization of bandwidth. Second, content distributors need vehicles to enable them to reach out to the masses of consumers, and to distinguish themselves from other distributors and content owners by means of new promotion and dissemination channels. Finally and most importantly, any new distribution platform must be equipped with digital rights management capabilities that enforce usage conditions specified by content owners and producers, and prevent any illegal usage, such as making unauthorized copies, of the content.

In this paper, we presented a complete end-to-end system for scalable distribution of copyright protected content. Scalability is achieved by using digital broadcast networks for transmitting the large content packages to multiple clients simultaneously. This broadband distribution model achieves efficiency in bandwidth utilization while minimizing the download time latency. The system utilizes the penetration power of TV to open new interactive promotion and dissemination channels for content distributors, in a way that is effective in reaching a broad base of consumers. The downloaded content is maintained constantly encrypted, and its usage is stringently controlled by a digital rights management system. Finally, it was shown how the system adapts to situations where back channel connections to a clearinghouse are expensive or not always available, and how the system's promotion and content dissemination channels may be split over a combination of unicast and broadcast connections.

The work presented in this paper is currently being incorporated into IBM's EMMS [EMMS] for scalable distribution of copyright protected material over satellite and cable digital video broadcast networks.

References

[Aksoy99] D. Aksoy, and M. Franklin, "Scheduling for large-scale on-demand data broadcasting", *Proc. of IEEE Infocom*, San Francisco, CA, pp 651-659, March, 1998.

[Brass99] J.T. Brassil, S. Low, N.F. Maxemchuk, "Copyright protection for the electronic distribution of text documents", *Proceedings of the IEEE*, 87(7), pp. 1181-1196, July 1999.

[Choud95] A. Choudhury, N. Maxemchuk, S. Paul, and H. Schulzrinne, "Copyright protection for electronic publishing over computer networks", *IEEE Network*, May/June 1995.

[CG] ContentGuard, http://www.contentguard.com

[DirecPC] Hughes Network Systems' DirecPC, http://www.direcpc.com

[EMMS] IBM's Electronic Media Management System, http://www.ibm.com/software/emms

[Intertrust] Intertrust's Metatrust system, http://www.intertrust.com

[Intercast] Intel's Intercast system, http://www.intel.com

[Kohl98] U. Kohl, J. Lotspiech, and S. Nusser, "Security for the digital library – protecting documents rather than channels", *Proc. of the IEEE 9th Intl. Workshop on Database and Expert Systems Applications*, 1998.

[Low00] G. Lowton, "Intellectual property protection opens path for e-commerce", *IEEE Computer*, February 2000.

[Mour01] M. Mourad, J. Munson, G. Pacifici, and A. Youssef, "An infrastructure to support Web content protection", *Submitted to the 10th International World Wide Web Conference,* Hong Kong, China, May 2001.

[MPEG] Motion Picture Expert Group, ISO/IEC JTC/SC29 WG11, http://www.cselt.it/mpeg

[SDMI] Secure Digital Music Initiative's Portable Device Specification, http://www.sdmi.org, July 1999.

[Stei95] R. Steinmetz, and K. Nahrstedt, "Multimedia: computing, communications, and applications", Prentice-Hall, 1995.