Domain Management System for Educational Services using Digital Broadcasting via Home Servers

1. Introduction

Digital broadcasting is steadily increasing in popularity in terms of both satellite and terrestrial broadcasts. "High-definition TV" has dramatically increased the expressive capabilities of digital TV, but by incorporating "Server-based broadcasting," digital televisions are expected to become "comprehensive information terminals" that offer users easy access not only to broadcasts but to information from communication routes as well.

In preparation for the implementation of server-based broadcasting, the "Server-based broadcasting operating regulation creation project" (the "Server Project") was established in September 2003 to promote studies on operating regulations and receiver specifications. Services are expected to begin by 2007. Figure 1 shows an outline of trends in the standardization of server-based broadcasting.

NHK is currently studying "Broadcasting-based Education Services" as one example of an attractive server-based broadcasting service. The advantage of server-based broadcasting is that it can utilize interactive contents, so students can use contents freely in their studies, according to their own level of understanding. These contents are designed to be easy to understand visually, and so are useful in further increasing the students' understanding. In order to achieve Broadcasting-based Education Services using server-based broadcasting, the schools must have multiple receiver terminals connected to a network, and these terminals must enable the users to freely view, edit, and store educational contents.

In the context of this usage method, however, there are some contents that are limited to school education. For this reason, we have developed a method that allows contents limited to in-school applications to be used freely, and we have conducted tests of prototype equipment using this method. Here, we will refer to the limiting of the scope of contents usage as "Domain Management."

In this paper, we will present an outline of Broadcasting-based Education services using the server-based broadcasting method that is currently being studied, and report on the Domain Management method that we have developed.

2. Studying with Digital Educational Materials

NHK is investigating "Digital Educational Materials" as one aspect of Broadcasting-based Education services. One unique feature of this system is that a digital TV is used in place of the blackboard used in a regular school classroom. Digital educational materials can be used for a variety of study formats, including the new "Integrated Study" classes.

Figure 2 shows an example of the contents of digital educational materials. Figure 2(a) is the home page. When the user selects "Make Reservation," the reservation page (2(b)) is displayed. On this page, the button for reserving the program that contains educational materials for 4th grade (in elementary school) is shown as an icon. By selecting this button, the user can make a reservation to record the series.

If the user selects the "My Blackboard" button on the page in Fig. 2(a), the "My Blackboard" page shown in Fig. 2(c) is displayed. On this page, the teacher can search for programs or clips (video programs 1-2 minutes in length)
and can use these contents in the lesson.

Next, when "View" is selected on the home page in Fig. 2(a), a list of programs and services is displayed. There are four types of services in this list: "Programs," "Clips," "Educational Materials," and "Bulletin Board." If "Outline" is selected under "Programs," the "Outline" page shown in Fig. 2(d) is displayed. This enables the user to view an outline of the broadcast program, or the program itself. The actual program is divided into several segments, and an outline of each segment has been prepared, so the user can select and play back the segments that are required. The "Clip" section contains a large number of program clips. Clips are broadcast in advance (for example, late at night), so if a recording reservation is made, the user can play back the desired video clip anytime. "Educational Materials" contains contents in a game format. The "Bulletin Board" provides teachers and students with a venue for exchanging ideas and holding discussions over the Internet.

3. In-school Domain Management Technology

With server-based broadcasting, it is possible, for example, to specify Rights Management & Protection Information (RMPI) for each set of contents. Examples of RMPI include: Contents usage period, number of uses, number of copies, and transfers of contents. This information is related to usage formats in regular households, but it also includes information that enables contents to be edited and used.

Figure 3 shows an example of how contents might be used in a school. Contents are stored in a "gateway," having been received via broadcast or communication routes. Receivers A, B, and C in the classrooms and teacher's room in this diagram are affiliated with the school's domain. These receivers are able to freely use the contents stored in the gateway, which is also included in the school's domain. If each of the receivers has a storage device, then users on one terminal can use contents stored on another terminal.

3.1 Domain Management Method

In-school Domain Management Technologies are required to enable broadcast contents that can be accessed by anyone to be used freely as educational materials in the limited context of school education based on RMPI.

In this method, the gateway installed in the school issues a School Certificate to the receivers in the school using an in-school domain device. The server-based broadcasting receiver has a server CAS (Conditional Access System) card function for authenticating the device and for protecting and managing broadcast contents. The CAS card uses four

Figure 3: Using Contents in a School
types of keys to encrypt and protect the contents after they have been stored. The receivers on the in-school domain use an extended CAS card with powerful security features and a function for storing the in-school certificate on the server CAS card, so that content usage is limited to in-school applications. Contents are encrypted and distributed from the gateway. The decryption key can only be received by a receiver with an in-school certificate. This system thus enables domain management based on RMPI.

3.1.1 Issuing of in-school certificates using PKI technology

The in-school certificate uses PKI (Public Key Infrastructure) technology. This technology uses public key encryption to create digital signatures and to authenticate devices. PKI is a commonly used technology, and can be implemented at a comparatively low cost. Public key encryption technology uses a pair of keys: one key is used for the encryption of regular text, and that encrypted text can only be decrypted using the other key in the pair. The unique feature of public key encryption technology is that even if you have access to one of the keys, it is impossible to calculate or deduce the other key; one key is a public key, and the other is a private key.

First, the gateway that issues the in-school certificate makes a judgment regarding validity as follows: The gateway has a gateway certificate, which contains a digital signature for the managing certification agency (e.g., a broadcasters’ organization). The digital signature can be used in conjunction with the certification authority to confirm validity.

The gateway then makes a judgment as to whether the receiver is valid, by checking the certification authority's digital signature on the receiver certificate, which is contained in the extended CAS card. If the receiver is valid, then the gateway issues an in-school certificate that includes the gateway's digital signature, which indicates the affiliation with the in-school domain. In the case of public key encryption, whenever an in-school certificate is issued, a matching private key is always created to form a pair.

The receiver stores the in-school certificate in the extended CAS card along with the private key. The private key is then used for the encryption of the key used to decrypt contents between the gateway and the receiver.

3.1.2 Distribution of content keys

Figure 4 illustrates an example of the distribution of the content key Kc in domain management. The content key for decrypting contents (Kc) is created using a common key encryption method. It is called a "common key" because it is the same key as the one used when encrypting contents. Kc is distributed via a broadcast, and is stored in the gateway. When contents are used on the receiver, Kc is distributed to the receiver in the following way. A "Session key" (Kg/a_session), which is common to both the gateway and the receiver, is created using private information from the gateway certificate and private information from the receiver's in-school certificate. Kc is distributed after being encrypted by Kg/a_session. Kc is distributed among the receivers using the same procedure. In this way, the contents can only be used by receivers that have received Kc. When the in-school certificate and the private key are distributed by the gateway, they are encrypted in the same way by the session key using the gateway certificate and the private information in the receiver certificate.

3.1.3 Protection of metadata

Here, we will provide an explanation of the "digital signature," which protects metadata from being tampered with outside of the school domain.

Digital educational materials use "metadata," for example in the "My Blackboard" function described in section 2. The titles of clips and programs selected by the teacher, as well as the order of playback, are stored as metadata.

The receivers within the school domain insert an in-
Feature

NHK STRL

Broadcast Technology no.24, Autumn 2005 © NHK STRL

school digital signature into the metadata that is created. The receiver can limit the use and editing of metadata created by an in-school receiver to use and editing within the school domain by authenticating the in-school digital signature.

Figure 5 shows the process for embedding a signature in the metadata. By compressing the binary data from the XML text using a “hash algorithm,” a hash value unique to that metadata is created.

The hash algorithm makes it very difficult to back calculate to the original data, or to create the two original data components that generated the same hash value. This algorithm is thus ideally suited to use in digital signatures for confirming that data has not been tampered with.

After the hash value is created, it is encrypted using the private key contained in the extended CAS card to create the signature. The created signature and the in-school certificate are added to the metadata, so that the metadata cannot be edited outside of the receiver that created the respective values. The in-school certificate is added to the metadata to verify that the signature is valid.

3.2 Prototype equipment for testing of domain management

Figure 6 shows a block diagram of the prototype equipment. The students’ terminals and the teacher’s PC terminal are connected by a network. The Broadcasting-based Education contents are stored in the gateway, and can be accessed by issuing an in-school certificate to each of the terminals. Using this prototype domain management system, we confirmed the functionality of the domain management method described above.

4. Conclusion

According to the Ministry of Education, Culture, Sports, Science and Technology’s goals for incorporating information technologies into education, classrooms in all public schools will have high-speed internet access by 2005, and the use of these technologies in classes will be promoted. As part of this movement to bring information technologies into the classroom, NHK is working to create Broadcasting-based Education service contents for use in server-based broadcasting, and to enable practical applications of these broadcast contents.

We will continue to develop rich, advanced services with that combine broadcasting and communication technologies to promote the use of server-based broadcasting in schools, and to conduct research and development targeting content protection and management technologies that are appropriate to these applications.

(Kyohiko ISHIKAWA)