Effective Multiplexing Method for Conditional Access System in Terrestrial DMB

YongHoon Lee, Gwangsoon Lee, Jinhwan Lee, Chung Hyun Ahn, Soo In Lee, and Nam Kim

ABSTRACT—This letter proposes a conditional access system (CAS) suitable for use in terrestrial digital multimedia broadcasting (T-DMB), based on an effective multiplexing method to provide encrypted T-DMB services. Specifically, the proposed multiplexing method for a CAS is designed to reduce the additional bit rate while assuring easy access to the designated encrypted services. Finally, the performance of the implemented CAS is confirmed through implementation and a broadcasting experiment under various service environments.

Keywords—Terrestrial DMB, CAS, multiplexing.

I. Introduction

In terrestrial digital multimedia broadcasting (T-DMB), video services and data services are multiplexed into a digital audio broadcasting ensemble frame [1]-[4]; therefore, the conditional access (CA) process should be done at several protocol layers of T-DMB. The CA process in T-DMB is designed to select CA modes according to the transport protocol layers and characteristics of services, namely, subchannel CA, data group CA, and multimedia object transfer (MOT) CA as shown in Fig. 1 [5]. In addition to a scrambling process, several messages for CA service should be multiplexed into the main service channel (MSC) as shown in Fig 1. For instance, these messages which are generated from the CA system (CAS) encoder include an entitlement management message (EMM) that concerns the entitlements of a user, and an entitlement control message (ECM) that contains the current control word. In T-DMB, these kinds of messages are called CAS internal messages (CAIntMess). Also, several parameters are specified to let the receiver rapidly know some CA information transmitted through the fast information channel (FIC) of the ensemble frame. Therefore, it is important to effectively multiplex the CAIntMess with service, while minimizing additional data rates and assuring rapid access to the designated CA service.

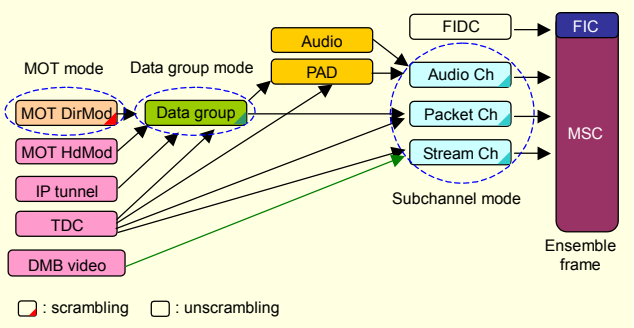


Fig. 1. CA modes according to transport layer of T-DMB.

II. Proposed CAS in T-DMB

1. Configuration of CA Transmission System

CA processing by existing specification [5] is done in front of the ensemble multiplexer in T-DMB transmission systems, which may cause several problems. CA processes, such as scrambling, generation of CA messages, and synchronization, could be needed at every service multiplexer. Accordingly, to solve such problems and to effectively apply a CA algorithm to each transport protocol layer according to CA modes, the CA operation needs to be done after managing all multiplexed services. To do this, we propose a CAS in T-DMB as shown in

Manuscript received May 27, 2008; revised Oct. 8, 2008; accepted Oct. 22, 2008.

YongHoon Lee (phone: + 82 42 860 3803, email: lee.h.y@etri.re.kr), Gwangsoon Lee (phone: + 82 42 860 1676, email: gslee@etri.re.kr), Jinhwan Lee (email: jinhwan@etri.re.kr), Chung Hyun Ahn (email: hyun@etri.re.kr), Soo In Lee (email: silee@etri.re.kr) are with the Broadcasting & Telecommunications Convergence Research Laboratory, ETRI, Daejeon, Rep. of Korea.

Nam Kim (email: namkim@chungbuk.ac.kr) is with the School of Electrical & Computer Engineering, Chungbuk National University, Cheongju, Rep. of Korea.

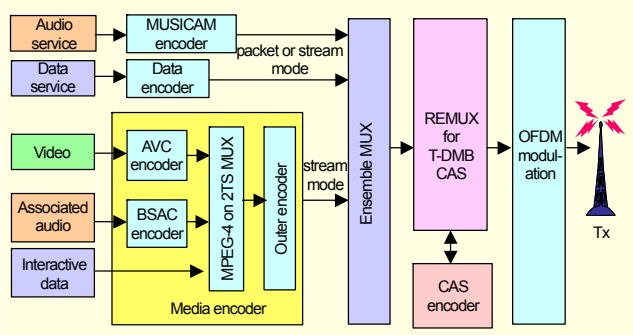


Fig. 2. Proposed CA transmission system in T-DMB.

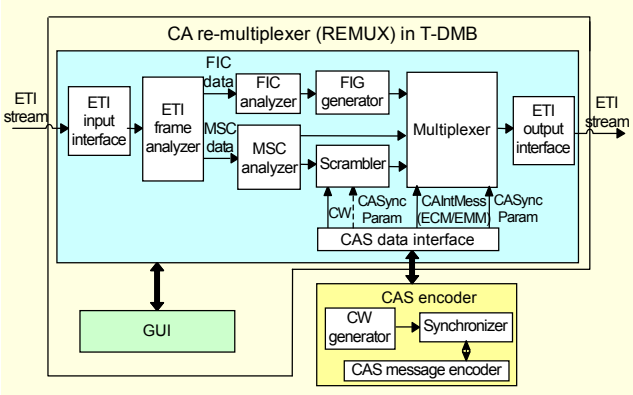


Fig. 3. Block diagram of CA REMUX in T-DMB.

Fig. 2. The proposed CA transmission system in T-DMB includes a CA re-multiplexer (REMUX), including a multiplexing function proposed in this paper, located at the next stage of the ensemble multiplexer. The CA REMUX includes the function of scrambling the data stream according to the CA mode chosen by a user. Only one scrambler can be used in the proposed system even if the CA process is selectively needed for several services at the same time.

2. Design of the CA REMUX in T-DMB

A block diagram of the designed CA REMUX in T-DMB is shown in Fig. 3. Some information to identify the transport protocol layers of services in the MSC stream is extracted from the FIC analyzer and transmitted to the graphical user interface. This information is used to set up the CA mode, and the FIC generator composes the fast information group (FIG) fields that deliver values regarding the service and CA information. The MSC analyzer categorizes subchannel data, which divides the MSC stream into three kinds of cases according to the CA mode.

The scrambler receives the control word and the CA synchronization parameters (CASyncParam) for synchronization with the descrambler. All kinds of messages and parameters for the CAS are generated by the CAS encoder. Finally, the

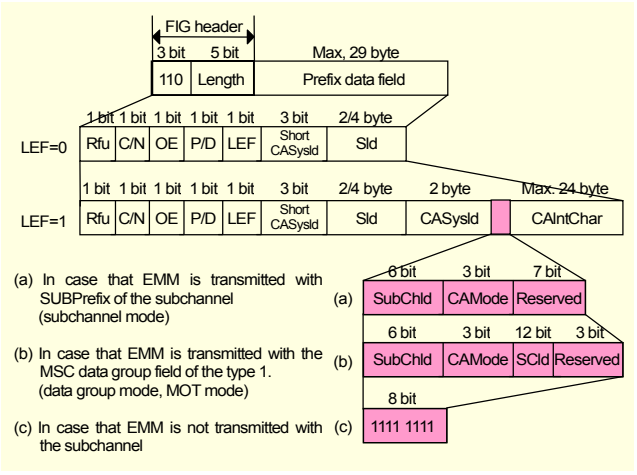


Fig. 4. Proposed structure of the FIG type 6 data field.

multiplexer multiplexes the scrambled stream, unscrambled stream, FIC data, and CAIntMess whose transporting positions are decided in accordance with the CA mode.

3. Multiplexing of CA Messages

T-DMB CA specifies that CAIntMess should be inserted into every service component for CA service as shown in section I. Among the CAIntMess, an ECM has to be transmitted for every service component to provide the scramble key to the CA receiver. However, inserting an EMM into every service component is likely to increase unnecessary overhead data. On the other hand, if an EMM is inserted into only one service component so as to reduce the overhead data, the CA receiver cannot easily access the service components that do not carry any EMM. In this section, we propose a solution to meet this requirement, which is to reduce the additional bit rate while assuring easy access to the designated encrypted service component. First, we propose extending FIG type 6 [5], which is a field to deliver signaling information concerning the CA service component, as shown in Fig. 4. We designed the CAS internal characteristics (CAIntChar) to carry necessary information by which the CA receiver can access a specific subchannel or MSC data group according to CA modes. Such a function can be performed at the FIG generator of the CA REMUX.

Figure 5 shows the configuration of the ensemble frame at the CA REMUX in the subchannel mode. The subchannel data composing the ensemble frame is scrambled after the CA operation previously described. Herein, the subchannel conditional access prefix (SUBCAPrefix) that transports the CAIntMess including ECMs or EMMs is attached at the head of the subchannel area in order to assure easy synchronization with the corresponding service. In Fig. 5, the CAIntMess is

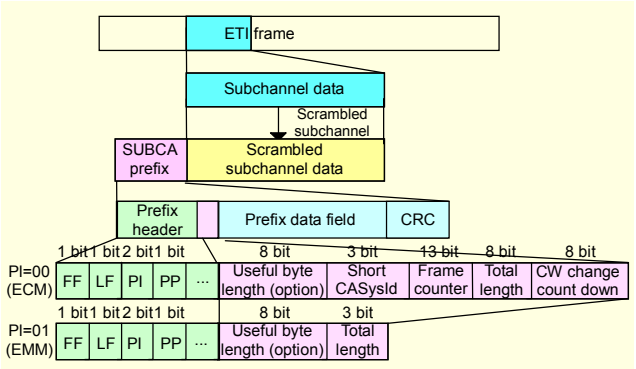


Fig. 5. Configuration of ensemble frame in subchannel CA mode.

Table 1. Service configuration.

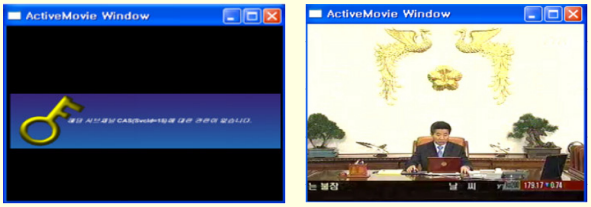
CA mode	Service category	Channel capacity	Protection rate
Subchannel	Video	544 kbps	3-A (1/2)
Data group	BWS	128 kbps	
MOT	BWS	128 kbps	

partitioned into packets within the SUBCAPrefix in consecutive frames. Therefore, a packet header is also defined to indicate the position of the packets. Among these headers, we propose PI (Packet Id) to indicate whether the prefix data field delivers an ECM or an EMM. If a SUBCAPrefix transmits an EMM, the position of the subchannel carrying this SUBCAPrefix is designated by FIG type 6 as shown in Fig. 4.

III. Experimental Results

We implemented the CA REMUX in T-DMB proposed in section II using a PCI card and software on an industrial PC, and we implemented a USB-type CA receiver including de-scrambling and DMB functions. To verify the developed CAS according to each CA mode, we set up the service configuration to include a video service and two broadcasting Web sites (BWS) [1] as shown in Table 1.

Figures 6 and 7 show screenshots of a player on the receiver after descrambling and decoding the services. As seen in Fig. 6, which corresponds to the subchannel mode CA, video service is ordinarily provided to users only when the authorized key that is created by the decoded CA parameters is used. Figure 7 shows screen shots of a BWS player, comparing MOT CA mode with and without the authorized key. The data stream can be ordinarily de-scrambled when the authorized key is used so that the BWS service is provided to user. Specifically, in MOT CA mode, only some object files that correspond to some of the HTML files in this example can be scrambled with the



(a) (b)

Fig. 6. Comparison of video service in subchannel CA mode: (a) without authorized key, and (b) with authorized key.

(a) (b)

Fig. 7. Comparison of BWS service in MOT CA Mode: (a) without authorized key and (b) with authorized key.

authorized key; therefore, only some text is ordinarily presented using the authorized key as shown in Fig. 7(a).

IV. Conclusion

In this paper, we proposed an effective multiplexing method to provide a variety of encrypted T-DMB services. We newly developed the CAS including the CA REMUX for T-DMB, which can encrypt the selected services according to the CA modes along with the CAS encoder. In the future, our research will be extended to develop an algorithm to deal with large amounts of data when there are high numbers of subscribers and events.

References

[1] ETSI EN 300 401, *Radio Broadcasting Systems: Digital Audio Broadcasting (DAB) to Mobile, Portable and Fixed Receivers*, v.1.3.3, May 2005.

[2] G. S. Lee et al., "A Novel Method for Inserting an MPEG-TS into Ensemble in a DMB Transmission System," *ETRI Journal*, vol. 26, no. 6, Dec. 2004, pp. 653-656.

[3] ETSI TS 101 498-1 v1.1.1, *Digital Audio Broadcasting (DAB): Broadcasting Website: Part 1: User Application Specification*, Aug. 2000.

[4] Sammo Cho et al., "Transmission of Traffic Information Using a Terrestrial Digital Multimedia Broadcasting System," *ETRI Journal*, vol. 28, no. 3, June 2006, pp 364-366.

[5] ETSI TS 102 367, *Digital Audio Broadcasting (DAB): Conditional Access*, v.1.2.1, Jan. 2006.