An Efficient and Flexible Hybrid Conditional Access System for Advanced T-DMB

Byungjun Bae, Yun-Jeong Song, Soo-In Lee, Hyung-Yoon Seo, and Jong-Deok Kim

This letter presents a hybrid conditional access system (CAS) for advanced terrestrial digital multimedia broadcasting (AT-DMB). The proposed architecture is characterized by its use of a unified CAS channel and various communication networks for CAS message transmissions. We implement a prototype CAS based on the hybrid architecture, which improves the CAS message transmission efficiency greatly compared to the existing T-DMB CAS standard and supports various AT-DMB interlayer services more easily and efficiently.

Keywords: AT-DMB, CAS, hybrid broadcast network.

I. Introduction

Terrestrial digital multimedia broadcasting (T-DMB) [1], a mobile-TV technology that is ahead of others in terms of market share, is now entering a new phase in Korea, where it was first developed and commercialized. The first part of this phase is the increasing demand for a new T-DMB business model [2]. While the estimated number of T-DMB users may be 30 million, operators still suffer from a deficit because they rely only on advertising for revenue. The second part is the development of advanced T-DMB (AT-DMB). AT-DMB doubles the spectral efficiency, while maintaining backward compatibility, by adopting hierarchical modulation. Operators can provide new services, such as high-quality video services based on scalable video coding (SVC), which are not feasible in T-DMB [3]. Many providers and other related bodies want to make use of AT-DMB in order to phase in a subscription-based service model, changing it from the current free service version. A conditional access system (CAS) is an essential technical enabler for this subscription-based service model. Actually, a CAS standard exists in T-DMB which was used in test services in countries, for example, Indonesia. However, we will show that there is a lot of room for improvement in the current standard on CAS message transmission efficiency.

As shown in Fig. 1, several conditional access (CA) parameters and messages are defined in the T-DMB CAS standard [4]. Parameters such as CAId and CAMode are included in fast information group (FIG) 0 and are used to indicate whether and how CA is to be applied in a service component (SC). CASysIdList is included in FIG 6 and is used to describe the applied CASs. Unlike CA parameters, CA messages such as entitlement control messages (ECMs) and entitlement management messages (EMMs) are included in the main service channel (MSC).

It is known that most CAS overhead comes from an EMM. While most CA parameters and messages are independent of the number of subscribers, an EMM is not. The number and

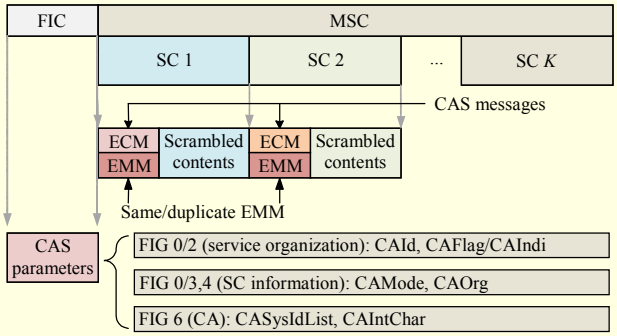

Fig. 1. T-DMB standard CAS parameters and messages.

Manuscript received Aug. 2, 2010; revised Oct. 1, 2010; accepted Oct. 25, 2010.

This work was supported by the KCC, Korea, under the "Test Support for AT-DMB Commercialization" support program supervised by the KCA (KCA-2011-10912-02004).

Byungjun Bae (phone: +82 42 860 3888, email: 1080i@etri.re.kr), Yun-Jeong Song (email: yjsong@etri.re.kr), and Soo-In Lee (email: silee@etri.re.kr) are with the Broadcasting & Telecommunications Convergence Research Laboratory, ETRI, Daejeon, Rep. of Korea.

Hyung-Yoon Seo (email: tanyak@mobile.cse.pusan.ac.kr) and Jong-Deok Kim (email: kimjd@pusan.ac.kr) are with the Department of Computer Science and Engineering, Pusan National University, Busan, Rep. of Korea.

doi:10.4218/etrij.11.0210.0320

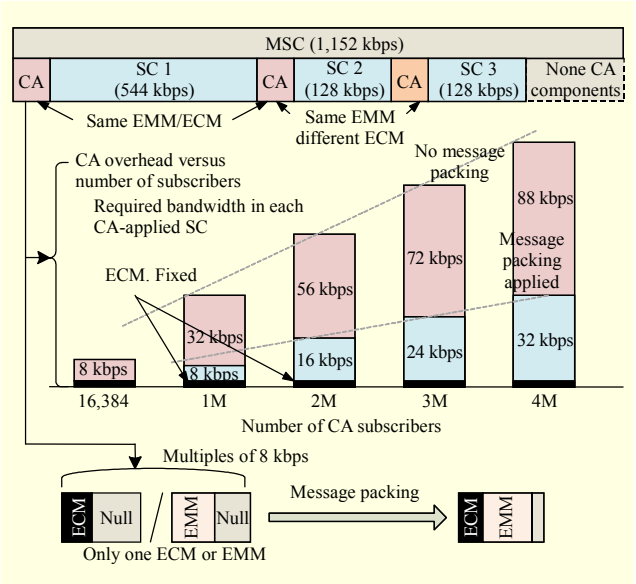

Fig. 2. Analysis results of CAS overhead using a raw stream.

size of EMMs increase as the number of subscribers increases. Efficient transmission of an EMM is crucial to realize a CAS that can support millions of subscribers. However, the standard specifies that an EMM should be inserted into every CA-applied SC. We think that this introduces unnecessary CAS transmission overhead because the same EMM may be sent several times.

To verify the aforementioned inefficiency problem, we analyze a raw stream generated by an existing commercial CAS that is built based on the standard. The raw stream is in ETI format and has three CA-applied SCs as shown in Fig. 2. To reduce CA overhead, it adopts a group-based encryption mechanism. One CA group consists of 16,384 subscribers, and most EMMs are generated and sent per group, not per subscriber. The stream covers only one group. For this one group, an additional 8 kbps is allocated in each SC. Even if we do not require all of the 8 kbps, we must allocate multiples of 8 kbps due to the multiplexing constraint of DMB [4]. We estimate the bandwidth required for CAS as the number of subscriber increases. As shown in Fig. 2, 32 kbps is required for 1 million subscribers and 88 kbps for 4 million subscribers in each SC.

However, we found that much of the allocated bandwidth is wasted as it transmits only one ECM or one EMM for one transmission opportunity. By applying this message packing method, we can decrease the required bandwidth from 32 kbps to 8 kbps for 1 million subscribers and from 88 kbps to 32 kbps for 4 million. Even with this enhancement, the EMM transmission overhead is far from negligible for large numbers of subscribers because of the duplicate transmission of EMM.

Although our goal is to design a CAS for AT-DMB, not for T-DMB, we are not free from this inefficiency problem of a T-DMB CAS because backward compatibility is one of the

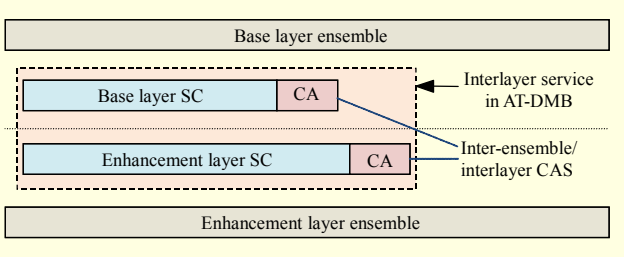

Fig. 3. Interlayer CAS in AT-DMB

key design principles of AT-DMB. However, it should be noted that there are technical challenges that are specific to AT-DMB.

In AT-DMB, operators are given two ensembles: an existing base layer and an enhancement layer. Though they are different ensembles, operators hope to make use of these two layers together to provide special services, such as SVC services, for AT-DMB subscribers that are not accessible by conventional T-DMB users. In an SVC service, the base stream is sent through the base layer and the enhancement stream is sent through the enhancement layer. AT-DMB CAS should support this interlayer service. Though two SCs are transmitted in different layers, CA procedures should be able to process them together. If we adopt the existing method as shown in Fig. 3, a duplicate CAS message transmission problem occurs and the complexity of synchronization in the descrambling process increases.

II. Proposed CAS Architecture for AT-DMB

We propose a hybrid CAS architecture characterized by its use of a unified CAS channel and various communication networks for CAS message transmissions. Its design goals include an improvement in CAS message transmission efficiency and flexible support of various CAS scenarios.

The unified CAS channel concept is depicted in Fig. 4. A separate DMB subchannel that includes all CAS messages for some SCs is defined as a unified CAS channel.

Although we illustrate only one CAS channel in Fig. 4, we do not restrict the number of CAS channels for flexibility. We also design it to support SCs in other ensembles. It can eliminate overhead due to duplicate transmissions of the same EMM. Moreover, as it supports components in other ensembles, interlayer CAS scenarios for AT-DMB interlayer services can be deployed more easily and efficiently. Realizing the unified CAS channel model needs a signaling mechanism that informs the CAS clients of the relation between a scrambled SC and its corresponding CAS channel. According to the DMB service structure, a service contains one or more SCs [1].

The essential component of a service is called a primary component, and the other components are called secondary components. In the unified model, scrambled media SCs may

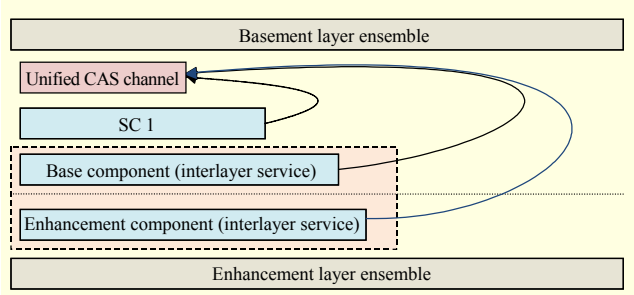

Fig. 4. Conceptual description of unified CAS channel.

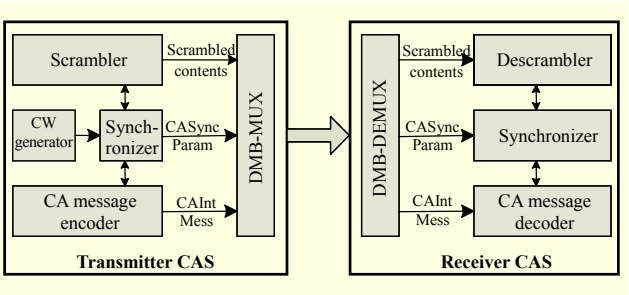

Fig. 5. Existing standard CAS architecture.

be considered a primary component and a CAS channel may be considered a secondary component. This kind of service organization can be signaled by multiplexing configuration information (MCI) signaling using FIG 0 and its extensions 2, 3, 4, and 8 [1]. Moreover, as in AT-DMB SVC services [5], it is possible to associate two components in different ensembles. Therefore, the unified model can also support interlayer CAS scenarios like the one shown in Fig. 4. To signal a proper CAS client module that can descramble CA-applied services, we use user application information, FIG 0/13. We want to emphasize that our unified CAS channel model can be realized without changing the current T-DMB signaling standard.

The other key architectural characteristic of our CAS is that it uses various communication networks, such as wireless Internet and a short message service (SMS), to transmit CAS messages. Figure 5 depicts the existing standard CAS architecture, and Fig. 6 depicts our CAS. In designing this hybrid architecture, we made an effort to develop a general framework and interface so that our CAS is not dependent on specific networks and protocols. To achieve this goal, we define CAS message manager (CMM) and CAS message agent (CMA) interfaces.

The CMM interface is defined for services between the CAS client module and CMM. One of the basic services of the interface is the request-and-reply of ECM/EMM. That is, when a client module needs an ECM/EMM for descrambling, it requests it from the CMM through the CMM interface, and the CMM replies by retrieving proper information from its CAS message DB. The CMA interface is defined for services between the CMM and CMA and developed to abstract or hide the difference in protocols for a CA message transmission in different networks. The CMA is defined for each specific network and protocol. A CMA on the server side encodes ECM/EMMs using its own specification and transmits it through its network, and the corresponding CMA on the client side has the opposite role.

Based on their temporal characteristics, CAS messages can be categorized into two classes: persistent and transient. Persistent messages are those that are frequently required by many subscribers, so CAS has to transmit them repeatedly in a proper interval. An ECM, which is indispensable for

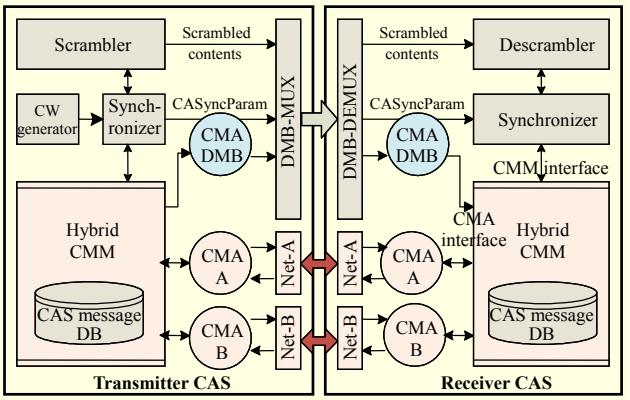

Fig. 6. Proposed hybrid CAS architecture.

descrambling, and some EMMs including an encryption key to decode the ECM are examples of persistent messages.

Transient messages are those that are usually required by a few subscribers for a certain time interval to carry out an action. Subscription-related EMMs are good examples of transient messages. In a broadcast-only CAS, as a server cannot know whether an EMM for a certain subscriber is received by the subscriber, it has to send the EMM repeatedly during a certain time interval. As the resources allocated for this kind of EMM are limited, if many subscription activities exist, perception of service quality may be fairly degraded. If a CAS cannot handle these dynamic transient messages effectively, advanced CA services such as pay-per-view will be difficult to deploy. The proposed hybrid architecture shows great improvement over existing architectures in handling dynamic transient messages.

III. Prototype System and Evaluation

We implement a prototype system to verify the feasibility of the proposed hybrid CAS architecture and to evaluate its transmission efficiency. It is implemented as a PC program, and Fig. 7 is a screenshot of the client program. In the prototype system, the server receives one audio and two video streams, scrambles them, and generates an ETI stream with proper CA information. We implemented three different CAS

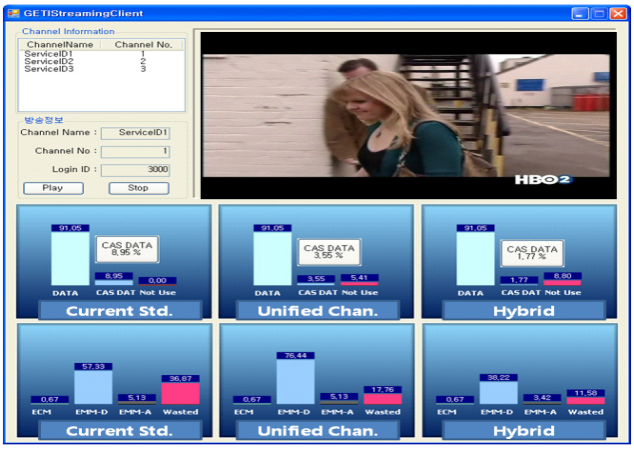

Fig. 7. Screenshot of CAS client prototype.

mechanisms. The first one emulates the existing system except that message packing is applied. The second one adopts the unified CAS channel model. The last one adopts the hybrid architecture as well as the unified channel model, and we implemented three CMAs, that is, CMA-DMB, CMA-IP (WLAN), and CMA-SMS, for it. The client receives the ETI stream and carries out descrambling by retrieving CA information for the selected CAS mechanism. The client displays the descrambled video and draws bar graphs showing how much DMB resources are used for CAS in each CAS mechanism. The overhead results are summarized in Table. 1.

Let $\Omega(t)$ be the amount of CAS messages that should be transmitted at time t. That is, $\Omega(t)$ is the overhead of CAS messages at time t. Conceptually, after some simplifications, $\Omega(t)$ of the existing standard can be represented as

$$\Omega(t) \cong \frac{ECM}{T_{\mathrm{ECM}}} + R \cdot \frac{EMM_{\mathrm{p}}}{T_{\mathrm{EMM}}} \cdot \frac{N}{G} + R \cdot EMM_{\mathrm{T}} . f(t), \qquad (1)$$

where $\Omega(t)$ consists of three terms: ECM, EMM_{P}, and EMM_{T}. EMM_{P} stands for persistent EMM, and EMM_{T} stands for transient EMM. N is the number of subscribers, G is the size of a group, and R is the number of CA-applied SCs. ECM and EMM_{P} are transmitted periodically, and T_{ECM} and T_{EMM} are the transmission intervals of each. $f(t)$ is the number of events that require transmission of EMM_{T} at time t. By its nature, $f(t)$ is random and hard to predict.

Note R in the second and the third term of (1). As mentioned earlier, the standard specifies that an EMM should be inserted into every CA-applied SC, so the overhead of EMM needs to be multiplied by R. However, R is removed from (1), that is, it is reduced to 1 in our unified CAS channel model. This enhancement is shown in the experimental results in Table. 1. Interestingly, the allocated bandwidth capacity of a unified channel should be large enough to accommodate $\Omega(t)$. However, it is not easy to determine a proper capacity due to the variety of $f(t)$. If $f(t)$ gets larger than predicted, the CAS channel gets congested and the CAS service quality will degrade. In our hybrid CAS architecture, this problem can be alleviated by making use of communication networks in transmitting EMM_{T}. If all EMM_{T} can be transmitted through communication networks, it will reduce $f(t)$ to 0 in (1). In the experiments of Table 1, we assumed that half of EMM_{T} can be handled through communication networks when the hybrid CAS architecture is applied and it shows the best results.

Table 1. CAS transmission overhead (kbps), R=3, G=16,384.

Number of subscribers (N)	Existing system	Message packed	Unified CAS channel	Hybrid
1 group	8×3	8×3	8	8
1 million	32×3	8×3	8	8
2 million	56×3	16×3	16	8
3 million	72×3	24×3	24	16
4 million	88×3	32×3	32	24

IV. Conclusion

In this letter, we proposed a new AT-DMB CAS architecture. It improves CAS message transmission efficiency greatly compared to the existing standard and supports various CAS services, including an interlayer CAS for AT-DMB. We also proposed a signaling mechanism for the architecture. As it utilizes the existing standard for backward compatibility, no new signaling specification is necessary.

For future work, we are focusing on introducing digital right management (DRM) into AT-DMB and integrating it with CAS. As in DVB-H, an integrated CAS/DRM architecture is necessary for seamless and efficient content protection in AT-DMB, so our research will be extended to that.

References

[1] ETSI EN 300 401, "Radio Broadcasting Systems: Digital Audio Broadcasting (DAB) to Mobile, Portable and Fixed Receivers," ver. 1.4.1, June 2006.

[2] Y.-J. Lee et al., "Design and Development of T-DMB Multichannel Audio Service System Based on Spatial Audio Coding," *ETRI J.*, vol. 31, no. 4, Aug. 2009 pp. 365-375.

[3] K.Y. Kim et al., "Efficient Generation of Scalable Transport Stream for High Quality Service in T-DMB," *ETRI J.*, vol. 31, no. 1, Feb. 2009, pp. 65-67.

[4] ETSI TS 102 367, "Digital Audio Broadcasting (DAB): Conditional Access," ver. 1.2.1, Jan. 2006.