A Study on the Entitlement Management for Digital Broadcasting System

Han-Seung Koo, Yoon-Jung Song, and O-Hyung Kwon
ETRI
{koohs, yjsong, ohkwon}@etri.re.kr

Abstract

Conditional Access System (CAS) performs entitlement management to make only legitimate subscribers watch pay-services. Generally, CAS uses passive entitlement management to fulfill that entitlement control, and various schemes are existed for that. Among them, Tu introduced two schemes in [1], which are the simple scheme and complete scheme of four levels hierarchy. The advantage of the simple scheme of four levels hierarchy is a small key generation and encryption load for a CAS, but it is not good for the dynamic entitlement management. On the other hand, the complete scheme of four levels hierarchy is good for the dynamic entitlement management, but key generation and encryption load for CAS is considerable when it is compared to the simple scheme. In this circumstance, we proposed a novel scheme, which is an active entitlement key management. The proposed scheme not only performs the dynamic entitlement management very efficiently, but also generates and encrypts keys with a small load for CAS, which is just the same as the load of the simple scheme.

I. Introduction

CAS based on hierarchic key distribution model refreshes keys regularly and irregularly [6]. First of all, CAS refreshes keys regularly because it provides key security and efficient billing. CAS performs efficient billing by synchronizing key refreshment period and service *charging time period* (CTP) [1]. However, since such frequent key refreshment causes a big system load, a trade-off between key security and frequent key refreshment is necessary. This regular key refreshment scheme is called *periodic entitlement management*. Second of all, CAS refreshes keys irregularly when extra key refreshment is necessary. For example, if a user wants to terminate his/her pay service or to change his/her current entitlement to another pay service before the entitlement is originally supposed to be expired, CAS performs irregular key refreshment. In this circumstances, CAS generally refreshes a key related to a channel or service group which a user wants to left, and periodically sends refreshed keys to all users except the one who left his/her entitlement. This irregular key refreshment scheme is called *non-periodic or dynamic entitlement management*. Note that CAS has to send keys periodically because all digital broadcasting standards [7]-[9] specifies one-way system as a mandatory requirement, and two-way system as an optional one. In other words, since CAS can원 assure a reception of refreshed keys at a host궐side in one-way system, there is no way but to send keys periodically for reliable key transmission. Unfortunately, this mechanism sometimes causes a big system load.

In [1], Tu proposed two kinds of *periodic* and *dynamic entitlement management*. First one is the *simple scheme of four levels hierarchy* [1] (we will call this scheme as the simple scheme in the rest of this paper) based on the *passive entitlement management* consists of *master private key*(MPK), *receiving group key*(RGK), *authorization key*(AK), and *control word*(CW). This scheme is the same as the three levels hierarchy, introduced in section I, except RGK and the fact that head-end CA server refreshes AK and RGK per CTP. Here, RGK is the unique key for each of *receiving group* (RG) [1]-[2], which is a group of subscribers who purchased the same package or channels. The second one is the *complete scheme of four levels hierarchy* [1] (we will call this scheme as the complete scheme in the rest of this paper) is proposed to resolve the problems of the simple scheme when CAS manages the dynamic entitlement. In this scheme, *the receiving group key* matrix, which has the size of M × N, where M and N is the number of charging group [1] and RG, respectively, is used.

An existing solution for *periodic* and *dynamic entitlement management* has a big flaw when it is applied to a big system with tens or hundreds *pay-per-channel* (PPC) and hundreds of thousand or millions of subscribers. That is a heavy system load for key generation and encryption [1]-[5]. Especially in case of *dynamic entitlement management*, system load problem is getting more serious because a probability of occurring extra entitlement status change events definitely will goes up compared to a small system. This problem is what we resolved with the proposed scheme. With an active entitlement key management proposed in this paper, CAS can handle *periodic* and *dynamic entitlement management* with a small load and securely, even though a system is huge.

II. An active entitlement key management

The proposed active scheme has four levels key hierarchy, such as MPK, RGK, AK, and CW. This key hierarchy model is exactly the same as the complete scheme, but the refreshment period of AK is not charging time unit(CTU), but CTP. Here, the CTU is the refreshing period of AK, and the duration of it could be 24-hour, generally. In the complete scheme, it has to refresh AK per CTU to support dynamic entitlement management because it is based on passive entitlement management scheme. How-ever, our proposed scheme broadcasts ARL to unauthorized subscribers to delete their invalid entitlement, so we don뭡need to refresh AK when a subscriber lefts his/her entitlement.

ARL is the list of the *record* which includes the identification code of an unauthorized subscriber. We can denote ARL as a group like {*record* 1, *record* 2, ? , *record* M}, where M is the time variant number which varies according to the accumulated number of unauthorized subscribers during a CTP. Each RG has its own ARL, and head-end CA server generates N ARLs, where N is the number of RGs, then broadcasts them to the associated subscribers. We