# 用户授权管理数据包时间域数据压缩策略研究

刘卫忠,冯卓明,周国学,邹雪城
(华中科技大学 电子科学与技术系,湖北 武汉 430074)

**摘 要**:通过对数字电视条件接收系统(CAS)中用户授权管理信息(EMM)的数据包结构的分析,在兼顾精度以及实用性要求的条件下,通过调整时间字段编码位长,可以有效压缩 EMM 数据包中的时间域信息的字节长度,减少 EMM 数据包长度,节省宝贵的带宽资源,提高用户授权信息的实时性,提升数字电视系统的用户体验。

**关键词**:数字电视;条件接收系统;用户授权管理信息;时间字段;时间域;数据压缩

**中图分类号**:TN949.197 **文献标识码**:A **文章编号**:1674-7720(2012)12-0090-03

## The study of time field data packet compression strategy of subscriber's entitled management message

Liu Weizhong, Feng Zhuoming, Zhou Guoxue, Zou Xuecheng
(Deptartment of Electronic Science&Technology, Huazhong University of Science&Technology, Wuhan 430074, China)

**Abstract**: This paper studied the conditional access system of digital TV and analyzed the entitled management message of CAS. To ensure the accuracy and practical requirements, a new strategy for compress the time item coded bit length have been proposed by adjust the time field coded bit length of EMM data, through the method, thereby reducing overall EMM packet length, saving valuable bandwidth resources, improve the subscriber's entitled speed and enhance the user experience of digital TV systems.

**Key words**: digital TV; conditional access system; entitled management message; time item; time field; data compression

数字电视条件接收系统是为了保证数字电视系统运营商的合法权益,通过对数字电视数字码流的加密和加扰,为数字电视安全运营提供技术保障。通俗地讲就是保证了只有付费或者即将付费的用户才能收看到所选择的节目,未付费者收看不到节目,从而保障节目提供商和运营商的利益。条件接收是现代信息加密技术在数字电视领域的具体应用[1-3]。

条件接收系统具体的实现原理是:包含视频、音频、数据的码流要在控制字的控制下进行扰码加密,将数据打乱后传输。控制字(CW)通常也称为密钥,由编码端加密后传送到终端接收设备,由智能卡来解密,恢复密钥即控制字。与控制字有关的加密信息通常称为授权控制信息(ECM)。对解密端所收看的多种业务进行授权的信息称为授权管理信息(EMM),也通过网络加密传送到终端接收设备。

## 1 数字电视条件接收系统整体架构

条件接收系统主要由产品授权及接口系统、数据库系统、ECMG 系统、EMMG 系统、加密系统、IC 卡管理系统、发卡系统、信息调度系统(EIS)、PSI/SIG/PDG 系统等模块构成[4-5]。系统结构如图 1 所示。

## 2 用户授权管理信息数据格式

EMM 消息为用户授权信息,采用产品密钥对用户的产品授权信息进行加密,并对加密后的密文和产品序号及当前时间使用分配密钥进行签名。该 EMM 内部数据结构包括消费产品号、时间、组密钥奇偶标识、产品奇密文、产品偶密文。组密钥奇偶标识为 1,表明对产品奇密文、产品偶密文采用奇组密钥加密;组密钥奇偶标识为 0,表明对产品奇密文、产品偶密文采用偶组密钥加密[6]。其结构如下:

```
EMM 授权段(EMM_AUTH_SECTION)语法结构{
    表标识
    版本号
    用户编号
    for(p=0;p<n;p++){
```

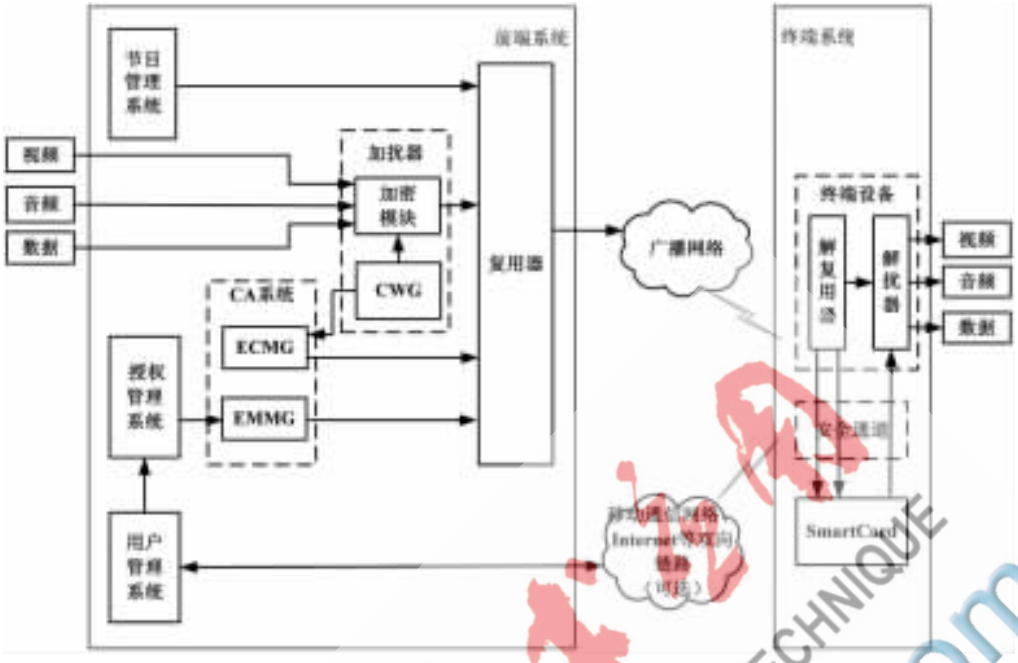


图 1 数字电视广播条件接收系统结构

产品信息
组密钥奇偶标识
加密后的奇产品密钥
加密后的偶产品密钥
产品授权时间信息密文
}
产品授权 MAC
}

其中，在 EMM 结构中用户的产品时间信息包括开始时间和结束时间，针对每个用户、每个产品其时间信息数据采用标准的 4 B 的 UTC 时间数据结构表述：

$L_{时间}=L_{开始时间}+L_{结束时间}$

故时间信息需要占用到 8 B 的空间。

假设网络中有 $N=300$ 万个订购用户，对于每一个用户、一个产品对应的数据报长度 $L$ 为：产品标识长度+开始时间+结束时间=1 B+4 B+4 B=9 B，假定用户平均产品数量为 $P=16$（在计算时取 16），故授权信息数据量为：

$D\_EMM=N\times L\times P=3000000\times 9\times 16=412$ MB

在 EMM 带宽为 512 kb/s 的情况下，寻址一轮所需时间为：

$T=D\_EMM\times 8/EMM$ 带宽 $=412\times 8\times 1024/512=6592$ s=1.83 h

也就是说，在 EMM 带宽为 512 kb/s 的情况下，用户授权更新需要 1.83 h，相当于用户订购产品后，平均需要 1.83 h 后才能收看，显然无法满足实时性的要求。

## 3 时间域压缩策略

如前所述，在系统注册使用用户不断增长的情况下，采用传统的时间数据格式，其数据量将越来越巨大，在用户量发展到一定的程度时，系统将不堪重负。

所谓的压缩算法，其实就是采用一定的模式将信息中的冗余信息进行合并，并可以将其中的一些微小数据量信息进行过滤。如前述，条件接收系统中用户授权时间信息采用 UTC 标准的 4 B 进行编码，基准单位为 s，可表示的时间长度为：

$T_{4B}=2^{4\times 8}=2^{32}=4294967295$ s=49710.2 d=136 y

在实际系统中，用户授权时间跨度一般不会超过 10 y，因此可以看出采用秒为单位计时有很大的冗余。而且作为广播式系统，基准计时单位也无需精确到秒级，分钟级的时间精度完全可以满足业务要求。由此可见，对时间域数据进行压缩是可行的。

(1)方案 1

根据以上分析，基于分钟级的时间精度的前提下，10 y 的大小为：

$T_{10y}=10\times 365\times 24\times 60=5256000<2^{23}<2^{24}$。故利用 3 B 的长度完全可以满足以分钟为单位的时间长度需求。此时，授权时间信息编码位长度为：

$L_{时间}=L_{开始时间}+L_{结束时间}=3$ B+3 B=6 B

该方案中一个重要的信息是系统授权基准时间 $\sigma_{系统}$，则终端恢复成标准时间的计算方法为：

$T_{标准开始时间}=\sigma_{系统}+T_{CAS\ 开始时间}$

(2)方案 2

在方案 1 的基础上进一步分析发现，在广播式网络中，用户订购的时间跨度一般以月为单位，授权时间长度以天为单位完全可以满足要求。在授权时间中包含信息格式为：$T_{CAS\ 开始时间}+T_{CAS\ 结束时间}$，采用以下格式：$T_{CAS\ 开始时间}+\lambda_{授权时长}$。其中时间长度采用以天为单位的格

式来表达，则其支持的最大时间跨度为：

$L_{2B}=2^{2\times8}=2^{16}=65535$ d=179 y。采用该格式完全可以满足业务需求。

采用方案2，时间信息长度为：

$L_{时间}=L_{开始时间}+L_{结束时间}=3\ B+2\ B=5\ B$

在此方案下，终端恢复为基于标准基准时间的结束时间为：

$T_{标准开始时间}=\sigma_{系统}+T_{CAS\ 开始时间}+\lambda_{授权时长}$

(3)方案3

上述结构中，进一步分析表明，如果将开始时间和持续时间结合在一起考虑，则可以发现：依据实际情况订阅节目的持续时间，一般来说，精度达到天已经绰绰有余了。通常订阅节目的时间很难超过3 y，即3×365=1 095 d，也就是说用$2^{10}$=1 024(约2.8 y)基本上就可以了，稳妥起见，可以用$2^{11}$=2 048(约5.6 y)表示，也就是说用11 bit去表示节目订阅持续时间，还可以保留5 bit扩展使用。

同时，订阅开始时间如果用2 B的话，最大可以表示65 536，如果计量单位采用小时，则可以表示大约7.5 y的时间(65 536/(365×24)=7.5)，显得略略不够精准，如果把订阅持续时间保留的5 bit扩展为订阅起始时间使用，则可以发现，总计可用21 bit表示订阅开始时间，$2^{21}$=2 097 152(约239 y/按小时计)，如果按照分钟计，可以表示约4 y的时间，如果按照两分钟为单位计，则可以表示8 y左右的时间，应该说与一般10 y左右的要求很接近了，也可以用在实际系统中。因此可以总结如表1所示。

表1 采用不同计量单位时的参数

| | 订阅起始时间 | 订阅持续时间 | 总计比特数 |
|---|---|---|---|
| 时间字段位长 | 21 | 11 | 32 |
| 可表达最大值 | 2 097 152 | 2 048 | |
| 按天计 | 5 745.62 | 5.61 | |
| 按小时计 | 239.40 | – | |
| 按两分钟计 | 7.98 | – | |
| 按分钟计 | 3.99 | – | |

采用方案3后时间信息长度为：

$L_{时间}=L_{开始时间}+L_{时间长度}=21\ bit+11\ bit=32\ bit=4\ B$

其中，开始时间计时单位为两分钟，持续时间计时单位为天。在此方案下，终端恢复为基于标准基准时间的结束时间为：

$T_{标准结束时间}=\sigma_{系统}+T_{CAS\ 开始时间}+\lambda_{授权时长}$

## 4 时间域压缩算法实现

在条件接收系统中，最大的信息量是用户产品的授权时间信息，对该数据进行压缩处理，可以有效提高整个系统数据传输的效率。其实对授权时间信息的压缩算法处理流程非常简单，基本流程简单描述如图2所示。

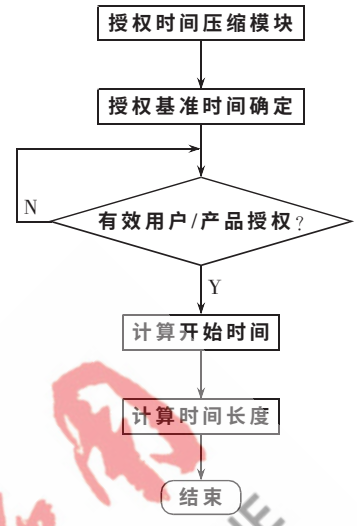


图2 授权时间压缩流程图

通过分析用户产品授权信息数据结构，提出了符合数字电视广播条件接收系统运营环境的对授权时间信息的压缩机制，包括开始时间的冗余信息压缩和结束时间的处理，使数据压缩比例可达37.5%($\eta=(1-\frac{5}{8})$)~50%($\eta=(1-\frac{4}{8})$)，有效地减少了数字电视条件接收系统中EMM授权信息数据量，提高了实时授权速度，节省了网络授权带宽。

参考文献

[1] 吴贤纶.有线电视前景分析[J].有线电视技术，2009(7)：3-4.

[2] 胡兵，吕广杰，叶梧.数字电视条件接收系统中密钥分配技术研究[J].中国有线电视，2005(Z1)：67-69.

[3] 木昌洪，刘卫忠，王旭升，等.基于DVB-C的条件接收系统的原理及其在机顶盒中的实现[J].中国有线电视，2004(2)：46-49.

[4] ETR A011r1：DVB common scrambling algorithm[S]. 2002.

[5] TU F K，LAIH C S，TUNG H H.One key distribution management for conditional access system on pay-TV system[J].IEEE Trans on Consumer Electronics，1999(45)：151-157.

[6] ETR A007:support for use of scrambling and conditional access with in digital broadcasting systems[S].2002.

(收稿日期：2012-04-24)

作者简介：

刘卫忠，男，1972年生，副教授，主要研究方向：网络通信与多媒体信号处理。