文章编号:1007-144X(2005)05-0249-04

数字电视有条件接收的研究和技术实现

朱耀光

(武汉理工大学 信息工程学院,湖北 武汉 430070)

摘 要:随着数字电视及相关业务的发展和应用,条件接收技术也越来越受到重视。系统地介绍了有线数字电视技术DVB-C中条件接收CA系统的组成框架、系统工作原理、安全密钥体系以及加扰技术、加密技术、及同密的概念等;重点结合数字电视条件接收系统工作实践,对条件接收技术在数字电视方面的应用作了分析和研究。

关键词:条件接收;加扰;加密;机顶盒;同密

中图法分类号:TN946.197 **文献标识码**:A

1 引 言

我国有线数字电视的发展速度和规模取得了长足进步,不仅音视频服务的质量得到了提升和丰富,而且随着网络双向改造完成,相关的增值服务,如视频点播(VOD)、数据广播和网上游戏等将得到逐步地开展。数字电视的发展为用户提供更加全面、优质的服务。而条件接收技术是有线电视增值服务的基础,为新业务的实现提供了一个安全、开放的环境。

条件接收从技术角度对收视者的合法权益、节目提供方和网络方的利益提供了支持和保证,使拥有授权的用户合法地使用某一项业务,而未经授权的用户不能使用这一业务。从国内外情况看,条件接收是广播电视事业向高层次发展的必由之路。近年来,条件接收系统已成为世界各国数字电视研究和开发的新热点。

2 条件接收系统简介

条件接收技术(Conditional Access)简称CA技术,是广播电视行业所使用的媒体保护技术。它将电视信号或其他数据在前端加扰,未授权用户无法收看或使用相关业务。授权用户(已经支付相关费用)可通过条件接收的终端部分收到已预订的电视节目和其他服务业务。

条件接收技术的核心部分主要由3大技术组成:加解扰技术、寻址技术和加解密技术[1]。

加解扰技术是指条件接收系统在发送端控制或改变被传送业务的某些参数来实现加扰,而解扰技术是将加扰信号还原成原始信号。在DVB-C标准中是采用了通用的由加扰序列来控制加扰的方法,由加扰序列对传输包进行扰动,方式包括按位异或及选取位取反等。

加解密技术是指对授权用户提供相关的信息和相关的过程进行加密。控制字(CW)的传输是CA技术的重要方面,采用多级加密、解密的体制确保CW的安全传输。

寻址技术是指向授权用户提供解扰的相关信息,使授权用户可使用解扰器解扰信号。未授权用户没有接收到解扰的相关信息,无法解扰。

3 条件接收系统的结构原理和技术

3.1 条件接收系统前端工作原理[2]

前端系统的结构图如图1所示。

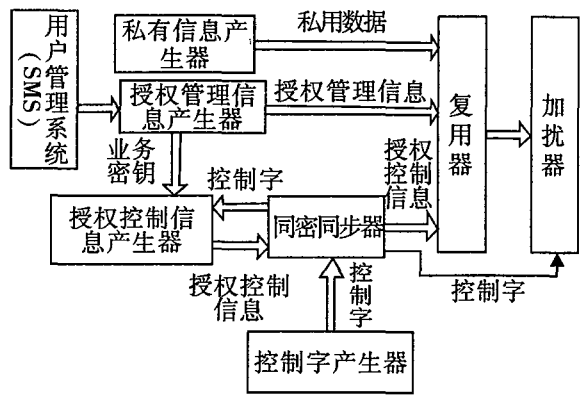

图1 条件接收系统前端图

收稿日期:2005-05-15.
作者简介:朱耀光(1980-),男,河北阳原人,武汉理工大学信息工程学院硕士研究生.
基金项目:武汉市重点科技攻关资助项目(20041001007).

控制字产生器(CWG)产生控制字(CW)对透明传输流(TS)进行加扰,控制字将提供给加扰器和加密器,前者的作用是对传输流进行加扰,后者使用业务密钥(SK)对控制字进行加密。使用业务密钥对控制字进行加密产生授权控制信息(ECM)。此ECM消息已经将CW及有关节目属性信息,如节目来源、节目时间、节目内容分类和节目价格等以密文形式封装到数据包内,通过同密同步器(SCS)同步,照特定的时序关系输入复用器。CA系统使用个人分配密钥(PDK)对业务密钥进行加密,产生授权管理信息(EMM),其中还包括用户管理系统发送的地址、用户授权信息等。复用器对音视频流、ECM和EMM等数据进行复用,经加扰器加扰通过ASI接口传送到调制器中,然后通过电缆传送到用户端,至此完成了前端的加扰控制工作。

3.2 终端系统工作原理[3]

接收端接收到已经加扰的TS流后,过滤出ECM和EMM消息,并按照一定的规则要求将ECM和EMM消息传送给智能卡。智能卡将授权写入智能卡的用户授权数据区,并根据授权条件及指定的密钥解出加扰控制字CW,同时将CW传送给机顶盒。机顶盒接收到CW后,将其传送给解扰器,如果解扰控制字CW正确,则可解出加扰节目,否则将收看不到节目。

4 同密技术

DVB标准中定义了同密加扰模式。同密要求前端可以使用多个CA系统,每个CA系统可以使用不同的加密系统加密各自的相关信息(CW、ECM、EMM等)。但对节目内容的加扰必须采用同一个加扰算法和加扰控制字。同密时,SCS模块起到非常重要的作用,它负责将加扰控制字传送给ECMG,同时负责调整各个ECM消息之间的时序,控制ECM与CW之间的同步关系等。这样可以保证接收端使用不同的接收设备而同时又能接收相同的数字电视节目。由此可见,使用同密技术后,可以方便多级运营商的管理,便于多级运营商灵活选择条件接收系统,如图2所示。

5 前端实现技术

在实现条件接收系统的工作中,为了使系统的安全性更高,加强对黑客的防范,同时使前端的操作具有实效性,提高系统的实用性,必须科学合理地设计和处理授权管理信息和授权控制信息。

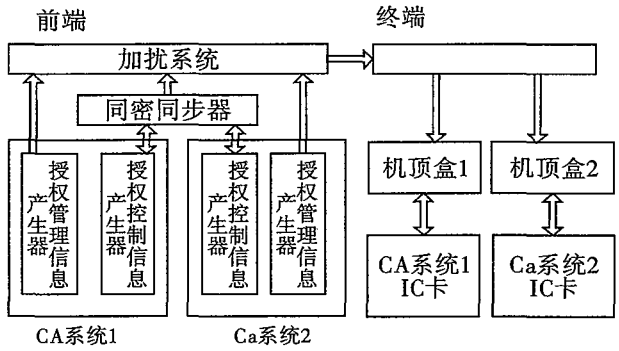

图2 同密结构图

5.1 授权控制信息(ECM)

ECM即授权控制消息,包含控制字CW信息,还包括如节目来源、节目时间、节目内容分类和节目价格等信息。由ECMG根据CW和EMMG传送来的业务密钥及相关的业务加密设置形成对应的ECM信息。系统可以对应每一个业务组(可以含一个或多个节目)均采用不同的CW,那么系统对应每个业务组均有独立的ECM。ECM中实现CW的加密传送。

ECM只与加扰产品或者服务的数目有关。由于在ECM中不传输与智能卡寻址有关的信息,所以与用户数目无关。加扰器产生控制字的能力和变化速率能使黑客无法长期获取和跟踪控制字。

大量频道加扰处理能力不仅仅依赖于CA系统自身并行发出加扰请求的能力,而且还依赖于加扰器产生控制字的能力和变化速率。DVB建议控制字的变化速率是5~10 s,这主要是考虑到安全因素,必须使控制字经常变化才能使系统安全。

5.2 授权管理信息(EMM)

由EMMG根据用户的授权信息以及其他信息,形成EMM信息。EMMG对ECM信息进行加密的密钥业务密钥(SK)进行管理,并完成EMM的注入。

EMM的数据量是CA系统的主要瓶颈,它的信息量越少占用带宽就越少,对用户数量的支持就越大。

EMM数据量(bit) = 发送的授权数量(每一张智能卡) × 接收该授权的智能卡数 × 平均EMM授权的数据量(bit)

EMM数据量的大小是由于CA系统本身设计的体系所决定的,因为EMM信息不仅包含有对节目授权的信息,还包含用户的寻址以及密钥等重要信息,由于在此基础上还要对这些信息加

密或数字签名,从而保证信息的完整性与安全性,而这一切又增加了 EMM 的信息量。从体系结构上讲它必须均衡考虑系统的安全性,将授权系统从根本结构上设计得非常精炼。在系统传输过程中,DVB 同密标准中定义了带宽协商的部分,EMM 的带宽是由复用器和 EMMG 协商决定的,实际应用中存在一个上限。EMMG 在整个传输过程中根据实际情况动态进行带宽请求,最大限度利用带宽。

EMM 的寻址方式同样也是提高系统性能的一个重要手段。CA 系统通过设置寻址信息可以非常灵活地对用户进行多种寻址。同时也可以达到压缩 EMM 数据量的目的,快速完成系统要求的对授权的操作,满足授权的实时的需要。

6 安全机制

CA 系统采用分层密钥加密系统[4]在密码学中,它已经成为一项公认的成熟的技术,安全性是不容置疑的。

6.1 多重加密体系

CA 系统的安全体系采用了多重加密体系[5]。利用控制字(CW)产生伪随机序列对原始 TS 流进行加扰,其结果是输出比特流扰码。在不解扰的情况下,接收端不能完成正常解码。利用业务密钥(SK)对 CW 进行加密控制,保证传输在网络中的 CW 不会被非法用户未经授权截获,从而对 TS 流进行解密。利用个人分配密钥(PDK)对 SK 进行加密,在这个层面上是寻址授权用户,确保非授权用户没有对业务密钥解密的权限,保证授权用户的利益不受损害,如图 3 所示。

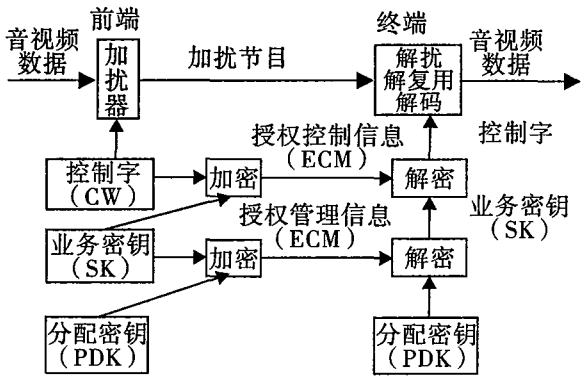

图3 多层加密解密图

6.2 常用加密算法简介

对于加密算法,有两类可选择:一类基于密钥的算法,加密的安全性完全取决于密钥的安全性;另一类是基于算法的加密,安全性是由算法本身的安全性所决定的。两类算法各有特点,第一类算法,由于算法安全性由密钥的安全决定,因此其加密算法可以公开并容易标准化,例如常见的 DES、IDEA、AES 和 RSA 等算法,但是安全密钥的产生、传送却变得尤为重要。对于第二类算法,需要保证算法本身不得泄露,否则安全性将受到威胁,但是可以采用更为复杂的数学计算保证其安全性。

6.3 密钥的更新频率、生命周期及算法的选择

控制字 CW 的更新频率为每 2 ~ 10 s 更新一次。对于控制字加密:要加密的数字电视信号数据量大,数据的价值较小,但对实时加密和解密的要求较高,要求算法不能太复杂,而加解密的速度和稳定性要求较高;有线电视传输网络是公开的,基本上是点对面的单向传输,所以是较不安全的网络结构,任何人都可以从中获取信息来分析研究。可以采用高效的单密钥算法,如 3DES 算法等[6]。

业务密钥(SK)是根据用户的付费条件对其进行更新,一般按月、季发送密钥,这个密钥的生命周期是 1 个月或数个月,也有按次(如 PPv,Pay - Per - View)或即时(IPPV,ImpulSe PPV)进行更新,这时密钥生命周期就只有几个小时。RSA 公钥加密算法应用较广。

个人分配密钥(PDK)通常保存在智能卡中,通过智能卡的 PIN 码进行保护,由于其加密强度高,智能卡通过 ROM、分区存储芯片内部数据等手段对其进行保护,因此 PDK 一般保持固定不变。

7 小 结

我国将进入电视技术的全面数字化,模拟电视将退出历史舞台,也就是说,现在的中国正处于一个技术更新与变革的时代。而条件接收技术为数字电视技术的迅速发展提供了一个安全、有序的平台。保证了用户、节目提供方和网络提供方三方的利益。

在技术实现层面,我国已经制定了相关的数字电视条件接收标准,国内的很多企业也研发了条件接收系统,在系统的安全性和实用性上取得了一定的成绩。随着技术的不断进步、数字电视业务的拓展,电视节目等媒体的传播途径不断增加,相应的保护技术应该可以面向具有知识产权

的节目细节,为节目细节提供完善、方便、实用的保护,在互动电视中对用户的主动创作进行知识产权保护,促进数字电视的发展。

参考文献:

[1] 穆长虹. DVB - C 条件接收系统[J]. 中国有线电视, 2004(19):18 - 21.
[2] 马正先. DVB 条件接收及其应用[J]. 中国有线电视, 2004(3):40 - 43.
[3] Hutchison M. Putting Conditional Access into Set - top Boxes[J]. IEEE Electronics Systems and Software, 2004(1):39 - 41.
[4] Liu B F, Zhang W J, Jiang T P. A Scalable Key Distribution Scheme for Conditional Access System in Digital Pay - TV System [J]. IEEE Transactions on Consumer Electronics, 2004(2):632 - 637.
[5] 陈文全,付国映,赵 利. 数字电视条件接收系统的安全性研究[J]. 中国有线电视,2004(2):6 - 9.
[6] 童廷洋,李 斌,杨会平. 数字条件接收的多层密钥系统[J]. 计算机工程与应用,2004(8):154 - 156.

Research and Technical Application of Conditional Access of Digital Televisions

Zhu Yaoguang

Abstract: The Conditional Access (CA) is paid more and more attention with the development and application of digital televisions and relevant business. The composition frame of CA system in cable digital technology DVB - C, operation principle of the system, the secure key system, the scrambling technology and encryption are introduced, including the concept of SimulCrypt. Combining with the practice and application on conditional access of digital TV, the technology application in conditional access on digital TV is analyzed.

Key words: conditional access; scrambling; encryption; STB; SimulCrypt

Zhu Yaoguang: Postgraduate; School of Information Engineering, WUT, Wuhan 430070, China.

[编辑:刘美玲]

(上接第 236 页)

Research and Implementation of Anticollision Principles of TYPE B Contactless IC Cards

Zhu Can, Liang Chuqiao

Abstract: The conception of contactless IC cards and the working principles of TYPE B Contactless IC cards are introduced. The basic principles of TYPE B anticollision protocols are analyzed. The anticollision protocols are implemented in contactless IC card chips; and the application proves that the system operates well.

Key words: contactless IC card; TYPE B; anticollision protocol

Zhu Can: Postgraduate; School of Information Engineering, WUT, Wuhan 430070, China.

[编辑:李道文]