(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103873895 A
(43)申请公布日 2014.06.18

(21)申请号 201210539322.4

(22)申请日 2012.12.14

(71)申请人 中国传媒大学
地址 100024 北京市朝阳区定福庄南里一号

(72)发明人 杨成 刘剑波 张雅琨 侯方天

(51)Int.Cl.
H04N 21/254(2011.01)
H04N 21/266(2011.01)
H04N 21/4623(2011.01)

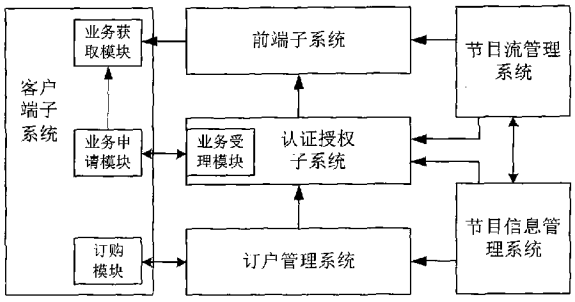
权利要求书3页 说明书15页 附图3页

(54)发明名称

一种 DVB/IPTV 双模互动业务保护系统

(57)摘要

一种 DVB/IPTV 双模互动业务保护系统，该系统包括客户端子系统、前端子系统、认证授权子系统、订户管理系统、节目流管理系统、节目信息管理系统部分，其中客户端子系统、CA 前端子系统、认证授权子系统为主要部分，订户管理系统、节目流管理系统、节目信息管理系统为外围辅助系统。该系统支持 DVB 和 IPTV 视频加扰，提供节目内容的可控加扰深度控制策略与自适应加扰、支持三种以上的密钥管理方式，128 位以上的密钥长度选择、大尺寸内容的分布式封装，具有对基于数字水印的内容安全与业务监管的支持。系统支持 DVB/IPTV 双模，引入密钥更新批处理策略以及分布式认证授权方案，提供百万用户规模的密钥实时更新与分配，降低了系统开销，增强了整个密钥更新的能力，提升了系统的安全性，为付费电视业务提供了灵活多变的保护机制。



CN 103873895 A

1. 一种 DVB/IPTV 双模互动业务保护系统，其特征在于：该系统包括客户端子系统、前端子系统、认证授权子系统、订户管理系统、节目流管理系统、节目信息管理系统部分、其中客户端子系统、前端子系统、认证授权子系统为主要部分，订户管理系统、节目流管理系统、节目信息管理系统为外围辅助系统，该 DVB/IPTV 双模互动业务保护系统，包括业务保护 CAServer 服务器、授权管理 DRMServer 和客户端 STB 中的 CAClient 三部分模块，其中 CAServer 服务器对应前端子系统，授权管理 DRMServer 对应认证授权子系统，客户端 STB 中的 CAClient 模块对应客户端子系统。

2. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：客户端采用分层和模块结构，客户端从上到下分为接口层、控制层和业务层；接口层提供标准的任务接口，接收用户业务指令及用户信息，接口层向用户反馈系统执行结果或解扰后的节目内容；控制层负责管理业务模块列表，根据业务指令调用相应的业务层模块完成相应的业务，协调各业务模块的运行，提供各业务模块的数据交流机制，并收集整理各业模块的执行结果反馈给接口层；业务层包括多个业务模块：订购模块、业务申请模块、业务获取模块；订购模块完成注册、购买、查询功能；业务申请模块完成节目单申请、点播申请、广播申请、直播申请、协商密钥功能；业务获取模块完成解复用、解密 ECM、解扰节目流、验证节目合法性功能；其中，解复用功能采用传统 DVB-CA 系统中奇偶控制字方式与前端子系统建立同步，并接收、解复用，获得 ECM 和节目流；解密 ECM 功能使用协商的会话密钥对 ECM 进行解密获得解扰控制字 CW；解扰节目流功能使用解密得到的控制字 CW 调用 AES 或 CSA 解扰算法对节目流进行解扰，将得到的 DVB/IPTV 节目流传输给控制层；验证节目合法性功能用于提取节目流中的合法性标识水印。

3. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：所述的前端子系统包括：控制字生成器 (CWG)、ECM 生成器 (ECMG)、水印嵌入算法 (WEA) 和通用加扰算法 (CSA)；前端子系统的作用是生成控制字，调用 CSA 对来自节目流管理系统的节目内容进行加扰；前端子系统的控制字发生器以系统密钥为基础生成控制字，采用 DVB 通用加扰算法 (CSA) 对来自节目流管理系统的节目内容进行加扰操作；前端子系统同时也使用会话密钥对控制字进行加密生成传统的 ECM；加扰后的节目内容与 ECM 传递给节目分发系统进行复用传输；前端子系统将以固定间隔重新生成加扰控制字，保证节目内容的传输安全；在点播交互模式下，前端子系统同时也负责接收用户的播放控制信息，并对加扰和节目流传输进行调整，所述的前端子系统进一步由实时封装子系统、预封装子系统、安全存储子系统构成，实时封装子系统用于对节目内容的实时在线封装与保护，预封装子系统用于对节目内容的离线封装与保护，实时封装子系统与预封装子系统可以根据需要选择其中之一使用或者共同使用，安全存储子系统可以根据需要选择使用。

4. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：所述的认证授权子系统由业务受理模块、业务密钥 SK 更新模块、双向认证协议、SK 协商协议、计时器、在线用户列表部分组成，认证授权子系统接受用户对节目内容的申请，通过认证和协商得到业务密钥 SK，并周期性的进行密钥更新，认证授权子系统的业务受理模块为与用户的接口，根据用户的节目申请启动相应的业务流程，在用户管理系统的配合下对用户的申请及其身份信息、信用信息进行合法性和有效性验证，对于合法、有效的申请，认证授权子系统提供密钥协商机制与用户协商获得会话密钥，并将会话密钥及其相关节目信息通过安全信

道发送给前端子系统系统，认证授权子系统将以固定间隔重新对用户的身份进行验证和重新生成业务密钥。

5. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，，其特征在于：所述的 CAServer 服务器包括接收端口、发送端口、解扰器、密钥端口四部分；所述的授权管理 DRMServer 包括 CA 端口、STB 端口、认证与链接管理模块、节目密钥管理模块和控制模块；所述的 CAClient 模块包括解扰器和密钥端口两部分，按层次划分为控制层、业务层，业务层是核心层，实现用户的登记注册、业务授权信息获取、节目的解扰功能。

6. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：该系统设计了密钥分发中心 (Key Distribution Center，KDC) 为客户端的加解密文件提供业务密钥，密钥分发中心先获得客户端密文文件的分割情况，当为 n 个子文件时，生成相应的 1 至 n 不重复的随机序列，客户端根据随机序列依次向存储服务器发送密文子文件；存储服务器建立新文件，将收到的密文子文件写入新文件，直至密文子文件发送完毕。

7. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：该系统使用了可控加扰深度策略与自适应加扰技术，根据运营商网络状况、不同压缩编码和码率动态调整加扰参数，能在保护业务的同时，减少数据处理量，减少了视频的加扰开销，该系统为实现对加扰深度的控制，对 I 帧和 I- 宏块的计数方法采用双上限计数 (n1，n2) 的方法，使得计数上限 n 值都可用和任意加扰深度 d 都可以选择；对任意的 d，如果：1) 1/d 为整数，则令 n1 ＝ 1/d，n2 ＝ 1；2) 1/d 不是整数，则将 d 表示为分式，并用欧几里德算法得到分子分母的最大公约数 r，约后得 d ＝ a/b，令：$\begin{cases} n1 = \lfloor b/a \rfloor \\ n2 = b \end{cases}$。

对找到的 I 帧计数 c1，c2，当 c1 达到上限 n1 时，对当前帧执行加扰操作；当 c2 达到上限 n2 时，两个计数器都清零，c1 ＝ c2 ＝ 0；

在应用中提供两种加扰深度的设置方式：1) n 方式设置，n 为加扰上限，实际设置加扰深度为 1/n；2) d 方式设置，d 为加扰深度，加扰上限 n 值采用上述的双上限计数方法确定。

8. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：该系统对高清互动大尺寸节目内容进行封装的效率问题，基于智能代理的分布式预封装技术，通过智能化的分割、调度、协同，在保证安全性和一致性的前提下，提高了对大尺寸节目内容的预封装速度，系统模型采用 C/S 结构，预封装系统端是服务器，视频输入是客户端，在预封装系统内部也使用 C/S 模式，由主服务器和代理服务器组成，代理服务器对主服务器来说是服务器端，主服务器是客户端；对需要封装加密的视频，首先进入主服务器，主服务器根据视频大小进行判断，选择是否需要代理服务器封装；若不需代理执行，则不分割视频文件，主服务器直接进行封装加密；若需要代理执行，则将视频文件根据设计的算法均分为几小段，然后自动搜索网络上的空闲代理服务器，将已分段的视频传送给可用的代理，让其执行封装功能；代理服务器封装完成之后，再及时返回给主服务器端，由主服务器端将返回的分段进行重组，恢复成一个完整的已封装好的“原视频”文件。

9. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：该系统运用了动态密钥更新与分配技术；动态密钥更新与分配分为两个阶段，分别是业务密钥交换阶段和动态业务密钥推送阶段；认证授权子系统与客户端的业务申请模块通过密钥协商协议产生业务密钥 SK；在成功协商密钥后，用户信息及其对应的业务密钥 SK 将被保存到在线用

户列表，计时器被启动；当到达指定时间间隔时，由业务密钥 SK 更新模块对在线用户列表中的用户重新进行认证和密钥协商，更新会话密钥 SK，其中，业务密钥 SK 采用 SSL 方式通过安全信道进行分发；除业务密钥 SK 外，该系统中还包含控制字 CW 和系统密钥 MK；其中控制字 CW 的更新与用户无关，按指定间隔进行更新。

10. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：系统在更新业务密钥的过程中，分别采用了密钥分级更新和组密钥更新；所述的密钥分级更新，即 DRM 授权认证系统在进行密钥更新时，上一级 DRM Server 只对本区内的 DRM Server 进行密钥更新，而不直接对用户提供服务，而组密钥更新是将广播业务和其他增值业务进行区别对待，如果用户已经订购了指定的广播业务，那么在切换使用其他业务时，DRM 授权认证系统不对广播业务密钥更新，只对增值业务进行密钥更新处理，在密钥更新的过程中寻找组密钥更新的最少节点。

11. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：该系统在前端子系统的预封装模块中加扰模块采用 CSA 和 AES 两种算法，根据环境需要实时改变加扰算法，加密模块采用 AES 算法对 CW 加密，支持 CBC（反向块链接模式）、OFB（输出反馈模式）、CFB（密码反馈模式）、CTR（技术模式）、ECB（电子密码本模式）五种加密模式对授权控制信息 ECM 进行加密，在前端子系统配置参数结构体中任意选取，实现了信息流的保密传输。

12. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于：该系统采用双层加密策略，包含两个加密层次，即单节目相关层 (PRL：Program Related Layer) 和业务相关层 (SRL：Service Related Layer)，PRL 层实施基于控制字 CW 对视频内容的加扰，SRL 层基于业务密钥通过加密生成业务相关控制信息 (SRI：Service Related Information)，即授权控制信息 ECM，加扰以控制字 CW 为密钥，调用通用加扰算法 CSA 完成对欲传输节目内容的直接加扰保护，加密以业务密钥 SK 为密钥，调用加密算法，对控制字 CW 的加密，形成授权控制信息 (ECM)，控制字 CW 保证节目内容的安全传输，同时控制字 CW 与业务密钥 SK 的分离，也使得节目内容的加扰与用户无关，降低了系统的复杂性。

13. 根据权利要求 1 所述的 DVB/IPTV 双模互动业务保护系统，其特征在于，该系统引入密钥更新批处理策略，使百万用户规模的密钥实时更新与分配，其包括一个授权服务器 (AS，Authentication Server) 和多个密钥服务器 (KS，Key Server) 两个部分，其中授权服务器作为树根，分发业务保护的关键信息，并通过密钥服务器管理间接管理所有用户；授权服务器，包括用户认证模块、密钥服务器模块以及用户授权模块，授权服务器通过 SSL 安全信道接收用户的接入或离开请求，并对用户进行身份认证；密钥服务器，包括密钥生成模块、密钥分发模块以及密钥管理模块，密钥服务器通过密钥生成模块产生伪随机数，作为待分发的点播业务密钥；由密钥分发模块实现针对授权组成员的组密钥分发；密钥管理模块与授权服务器进行数据交互，在授权服务器发出添加或删除指定成员的指令时，密钥管理模块通知密钥生成模块产生新的点播业务密钥，然后密钥管理模块将经过更新后的点播密钥发送给授权服务器，并由密钥分发模块对指定的用户密钥节点进行密钥更新。

一种 DVB/IPTV 双模互动业务保护系统

技术领域

[0001] 本发明涉及信息安全领域，具体地说，是涉及宽带互动电视系统双向非对称数字电视系统的关键技术。

背景技术

[0002] 在 iDTV（互动数字电视）、IPTV（交互式网络电视）等互动视频系统的建设发展中，互动视频业务内容的保护与控制正成为影响互动视频业务得以推广的重要瓶颈，其涉及内容保护、传输保护、访问控制、盗版追踪和内容监控等方面的技术。

[0003] 传统的视频业务保护系统建立在单向网络上，为了将加扰控制字、用户的授权信息和管理信息等重要内容全的传输到客户端，采用了层层设防的基本思想，系统结构复杂，安全性不高，容易被黑客破解。

[0004] 由于传统的广电网属于广播网络，决定了其视频业务保护系统也必然是广播方式。在这种方式下，服务前端不了解客户端的状况，无法对客户端的有效性和可靠性进行验证，客户端也无法验证前端的有效性和可靠性，只能被动的接收，这与视频业务保护系统针对用户及其收看行为进行节目收费的初衷存在矛盾。

[0005] 在传统的视频业务保护系统中，前端对所有用户生成可能需要的安全信息加密并加以传输，一方面增加了网络负载，浪费大量带宽，给用户体验带来了较大的延迟，另一方面又因为大量加密信息的存在，增加了破坏者破解加密体制的可能性，形成潜在的安全隐患。

[0006] 传统的视频业务保护系统采用复杂的多重加密作为其密钥分发机制，增加了实施的难度，容易产生安全漏洞。每增加一个密钥，对密钥的生成、分发、管理的难度就会有大幅度的提升。破坏者只要破坏其中的任何一个环节，就可以有效地摧毁整个系统，即使是采取多密码算法备份等辅助措施，也无法从根本上解决这个缺陷。

[0007] 传统互动业务保护系统是广播网络的计费系统，没有对用户的身份认证，不适合双向网络；内容数字化和因特网的开放性给盗版追踪和内容监控造成了很大的困难。

[0008] 对视频节目的保护一般采用两种方式：预封装方式和实时加密方式。当需要封装的视频节目较多或者视频较大时，由于 CPU 处理能力有限，节目封装效率较低。

[0009] 对于传统 CA 系统，视频源的采集与传输都采用明文的方式，对视频源的安全性造成威胁。另外，现有的存储方式，不论是直接存储还是接收文件加密存储，都存在安全隐患。

[0010] 普通的加扰技术无法实现对加扰深度的选择控制，不能区分重要和非重要信息，加扰强度往往过大，加扰效果不佳。

发明内容

[0011] 基于上述，本发明提出一种 DVB/IPTV 双模互动业务保护系统，一种 DVB/IPTV 双模互动业务保护系统，其特征在于：该系统包括客户端子系统、前端子系统、认证授权子系统、订户管理系统、节目流管理系统、节目信息管理系统等部分。其中客户端子系统、认证授权

子系统为主要部分，订户管理系统、节目流管理系统、节目信息管理系统为外围辅助系统。该系统包括业务保护 CAServer 服务器、授权管理 DRMServer 和客户端 STB 中的 CAClient 模块三部分，其中 CAServer 服务器对应前端子系统子系统，授权管理 DRMServer 对应认证授权子系统，客户端 STB 中的 CAClient 模块对应客户端子系统。

[0012] 所述的客户端子系统（简称客户端）采用分层和模块结构，客户端从上到下分为接口层、控制层和业务层；接口层提供标准的任务接口，接收用户业务指令及用户信息，接口层向用户反馈系统执行结果或解扰后的节目内容；控制层负责管理业务模块列表，根据业务指令调用相应的业务层模块完成相应的业务，协调各业务模块的运行，提供各业务模块的数据交流机制，并收集整理各业模块的执行结果反馈给接口层；业务层包括多个业务模块，包括：订购模块、业务申请模块、业务获取模块；订购模块完成注册、购买、查询功能；申请模块完成节目单申请、点播申请、广播申请、直播申请、协商密钥功能；业务获取模块完成解复用、解密 ECM、解扰节目流、验证节目合法性功能；其中，解复用功能采用传统 DVB-CA 终端与前端子系统建立同步，并接收、解复用，获得 ECM 和节目流；解密 ECM 功能使用协商的会话密钥对 ECM 进行解密获得解扰控制字 CW；解扰节目流功能使用解密得到的控制字 CW 调用 AES 或 CSA 解扰算法对节目流进行解扰，将得到的 DVB/IPTV 节目流传输给控制层；验证节目合法性功能用于提取节目流中的合法性标识水印。

[0013] 所述的前端子系统进一步由实时封装子系统、预封装子系统、安全存储子系统构成。实时封装子系统用于对节目内容的实时在线封装与保护，预封装子系统用于对节目内容的离线封装与保护。实时封装子系统与预封装子系统可以根据需要选择其中之一使用或者共同使用。安全存储子系统可以根据需要选择使用。所述的前端子系统包括：控制字生成器 (CWG)、ECM 生成器 (ECMG)、水印嵌入算法 (WEA) 和通用加扰算法 (CSA)；前端子系统的作用是生成控制字，调用 CSA 对来自节目流管理系统的节目内容进行加扰；前端子系统的控制字发生器以系统密钥为基础生成控制字，采用 DVB 通用加扰算法 (CSA) 对来自节目流管理系统的节目内容进行加扰操作；前端子系统同时也使用会话密钥对控制字进行加密生成传统的 ECM；加扰后的节目内容与 ECM 传递给节目分发系统进行复用传输；前端子系统将以固定间隔重新生成加扰控制字，保证节目内容的传输安全；在点播交互模式下，前端子系统同时也负责接收用户的播放控制信息，并对加扰和节目流传输进行调整。

[0014] 所述的认证授权子系统由业务受理模块、业务密钥 SK 更新模块、双向认证协议、SK 协商协议、计时器、在线用户列表部分组成，认证授权子系统接受用户对节目内容的申请，通过认证和协商得到业务密钥 SK，并周期性的进行密钥更新；认证授权子系统的业务受理模块为与用户的接口，根据用户的节目申请启动相应的业务流程，在用户管理系统的配合下对用户的申请及其身份信息、信用信息进行合法性和有效性验证；对于合法、有效的申请，认证授权子系统提供密钥协商机制与用户协商获得会话密钥，并将会话密钥及其相关节目信息通过安全信道发送给前端子系统系统，认证授权子系统将以固定间隔重新对用户的身份进行验证和重新生成业务密钥。

[0015] 所述的 CAServer 服务器包括接收端口、发送端口、解扰器、密钥端口四部分；所述的授权管理 DRMServer 包括 CA 端口、STB 端口、认证与链接管理模块、节目密钥管理模块和控制模块；所述的 CAClient 模块包括解扰器和密钥端口两部分，按层次划分为控制层、业务层，业务层是核心层，实现用户的登记注册、业务授权信息获取、节目的解扰功能。

[0016] 该系统设计了密钥分发中心 (Key Distribution Center，KDC) 为客户端的加解密文件提供业务密钥，密钥分发中心先获得客户端密文文件的分割情况，当为 n 个子文件时，生成相应的 1 至 n 不重复的随机序列，客户端根据随机序列依次向存储服务器发送密文子文件；存储服务器建立新文件，将收到的密文子文件写入新文件，直至密文子文件发送完毕。

[0017] 该系统针对可变带宽环境下对节目加扰和宣传的需求，设计实施了可控加扰深度策略与自适应加扰技术，根据运营商网络状况、不同压缩编码和码率动态调整加扰参数，在保护业务的同时，减少数据处理量，减少了视频的加扰开销。系统为实现对加扰深度的控制，对 I 帧和 I- 宏块的计数方法采用双上限计数 (n1，n2) 的方法，使得计数上限 n 值都可用和任意加扰深度 d 都可以选择；对任意的 d，如果：1) 1/d 为整数，则令 n1 ＝ 1/d，n2 ＝ 1；2) 1/d 不是整数，则将 d 表示为分式，并用欧几里德算法得到分子分母的最大公约数 r，约后得 d ＝ a/b，令：$\begin{cases} n1 = \lfloor b/a \rfloor \\ n2 = b \end{cases}$

[0018] 对找到的 I 帧计数 c1，c2，当 c1 达到上限 n1 时，对当前帧执行加扰操作；当 c2 达到上限 n2 时，两个计数器都清零，c1 ＝ c2 ＝ 0；

[0019] 在应用中提供两种加扰深度的设置方式：1) n 方式设置，n 为加扰上限，实际设置加扰深度为 1/n；2) d 方式设置，d 为加扰深度，加扰上限 n 值采用上述的双上限计数方法确定。

[0020] 该系统针对高清互动大尺寸节目内容进行封装的效率问题，设计实施了基于智能代理思想的分布式预封装技术，通过智能化的分割、调度、协同等手段，在保证安全性和一致性的前提下，提高了对大尺寸节目内容的预封装速度。该系统模型采用 C/S 结构，预封装系统端是服务器，视频输入是客户端，在预封装系统内部也使用 C/S 模式，由主服务器和代理服务器组成，代理服务器对主服务器来说是服务器端，主服务器是客户端；对需要封装加密的视频，首先进入主服务器，主服务器根据视频大小进行判断，选择是否需要代理服务器封装；若不需代理执行，则不分割视频文件，主服务器直接进行封装加密；若需要代理执行，则将视频文件根据设计的算法均分为几小段，然后自动搜索网络上的空闲代理服务器，将已分段的视频传送给可用的代理，让其执行封装功能；代理服务器封装完成之后，再及时返回给主服务器端，由主服务器端将返回的分段进行重组，恢复成一个完整的已封装好的“原视频”文件。

[0021] 该系统运用了动态密钥更新与分配技术；动态密钥更新与分配分为两个阶段，分别是业务密钥交换阶段和动态业务密钥推送阶段；认证授权子系统与客户端的业务申请模块通过密钥协商协议产生业务密钥 SK。在成功协商密钥后，用户信息及其对应的 SK 将被保存到在线用户列表，计时器被启动；当到达指定时间间隔时，由 SK 更新模块对在线用户列表中的用户重新进行认证和密钥协商，更新会话密钥 SK，其中，业务密钥 SK 采用 SSL 方式通过安全信道进行分发；除业务密钥 SK 外，该系统中还包含控制字 CW 和系统密钥 MK；其中控制字 CW 的更新与用户无关，按指定间隔进行更新。

[0022] 系统在更新业务密钥的过程中，分别采用了密钥分级更新和组密钥更新；所述的密钥分级更新，即 DRM 授权认证系统在进行密钥更新时，上一级 DRM Server 只对本区内的 DRM Server 进行密钥更新，而不直接对用户提供服务，而组密钥更新是将广播业务和其他

增值业务进行区别对待，如果用户已经订购了指定的广播业务，那么在切换使用其他业务时，DRM 系统不对广播业务密钥更新，只对增值业务进行密钥更新处理，在密钥更新的过程中寻找组密钥更新的最少节点。

[0023] 该系统在前端子系统的预封装模块中加扰模块采用 CSA 和 AES 两种算法，根据环境需要实时改变加扰算法，加密模块采用 AES 算法对 CW 加密，支持 CBC（反向块链接模式）、OFB（输出反馈模式）、CFB（密码反馈模式）、CTR（技术模式）、ECB（电子密码本模式）五种加密模式对授权控制信息 ECM 进行加密，在前端子系统配置参数结构体中任意选取，实现了信息流的保密传输。

[0024] 该系统采用双层加密策略，包含两个加密层次，即单节目相关层 (PRL :Program RelatedLayer) 和业务相关层 (SRL :Service Related Layer)，PRL 层实施基于控制字 cw 对视频内容的加扰，SRL 层基于业务密钥通过加密生成业务相关控制信息 (SRI :Service RelatedInformation)，即授权控制信息 ECM，加扰以 CW 为密钥，调用通用加扰算法 CSA 完成对欲传输节目内容的直接加扰保护，加密以业务密钥 SK 为密钥，调用加密算法，对控制字 CW 的加密，形成授权控制信息 (ECM)，CW 保证节目内容的安全传输，同时 CW 与 SK 的分离，也使得节目内容的加扰与用户无关，降低了系统的复杂性。

[0025] 该系统引入密钥更新批处理策略，使百万用户规模的密钥实时更新与分配，其包括一个授权服务器 (AS，Authentication Server) 和多个密钥服务器 (KS，Key Server) 两个部分，其中授权服务器作为树根，分发业务保护的关键信息，并通过密钥服务器管理间接管理所有用户 ；授权服务器，包括用户认证模块、密钥服务器模块以及用户授权模块，授权服务器通过 SSL 安全信道接收用户的接入（离开）请求，并对用户进行身份认证 ；密钥服务器，包括密钥生成模块、密钥分发模块以及密钥管理模块，密钥服务器通过密钥生成模块产生伪随机数，作为待分发的点播业务密钥 ；由密钥分发模块实现针对授权组成员的组密钥分发 ；密钥管理模块与授权服务器进行数据交互，在授权服务器发出添加（删除）指定成员的指令时，密钥管理模块通知密钥生成模块产生新的点播业务密钥，然后密钥管理模块将经过更新后的点播密钥发送给授权服务器，并由密钥分发模块对指定的用户密钥节点进行密钥更新。

[0026] 该系统有效的解决了本发明提出的技术问题。

附图说明

[0027] 图 1 是系统框架图 ；

[0028] 图 2 是客户端的基本结构图 ；

[0029] 图 3 是前端子系统的基本结构图 ；

[0030] 图 4 是认证授权子系统结构图 ；

[0031] 图 5 是系统总体模块结构图 ；

[0032] 图 6 是分布式预封装系统模型图 ；

[0033] 图 7 是密钥更新路径选择图。

具体实施方式

[0034] 本发明的 DVB 和 IPTV 互动业务保护系统包括客户端子系统、前端子系统、认证授

权子系统、订户管理系统、节目流管理系统、节目信息管理系统等部分。其中客户端子系统、前端子系统、认证授权子系统为主要部分，订户管理系统、节目流管理系统、节目信息管理系统为外围辅助系统。该系统包括业务保护 CAServer 服务器、授权管理 DRMServer 和客户端 STB 中的 CAClient 模块三部分，其中 CAServer 服务器对应前端子系统子系统，授权管理 DRMServer 对应认证授权子系统，客户端 STB 中的 CAClient 模块对应客户端子系统。

[0035] 参见附图 2，客户端子系统（简称客户端）的基本结构如下：客户端为机顶盒或 TV 提供透明的节目内容访问，根据用户提供的节目信息，负责与订户管理系统、认证授权子系统和前端子系统交互，获得解扰密钥，实施对加扰节目的解扰工作，实现有条件接收和有条件播放能力。客户端的订购模块与订户管理系统通过安全信道交互传递用户身份信息、用户信用信息等内容，完成注册、购买等功能，为用户提供查询其身份和信用信息的交互机制；客户端的业务申请模块与认证授权子系统的业务受理模块交互传递用户身份信息以及对节目、节目单、节目类型（点播、广播、直播）的申请，并负责与认证授权子系统协商生成业务密钥，传递给业务获取模块；客户端的业务获取模块对从前端子系统同步获取加扰的节目内容进行解密和解扰工作，并在点播交互模式下向 CA 提交用户的播放控制信息（快进、快退、停止等），实现对节目流的交互操作。

[0036] 客户端采用分层和模块结构，便于系统的更新和升级，以提高系统的兼容性和灵活性。客户端从上到下分为接口层、控制层和业务层。接口层负责提供标准的任务接口，接收用户的业务指令（如注册、订购、点播、广播、直播、快进、快退、停止等）及其相关信息（如用户的机顶盒号、身份证号、身份证书等），提交给控制模块。同时，接口层也负责向用户反馈系统执行结果或解扰后的节目内容。

[0037] 控制层负责管理业务模块列表，根据业务指令调用相应的业务层模块完成相应的业务，

[0038] 业务层划分为若干个业务模块，各业务模块完成相对独立的业务。主要的业务模块包括：订购模块、业务申请模块、业务获取模块。订购模块完成注册、购买、查询功能。申请模块完成节目单申请、点播申请、广播申请、直播申请、协商密钥功能。业务获取模块完成解复用、解密 ECM、解扰节目流、验证节目合法性功能。其中，解复用功能采用传统 DVB-CA 终端与前端子系统建立同步，并接收、解复用，获得 ECM 和节目流；解密 ECM 功能使用协商的会话密钥对 ECM 进行解密获得解扰控制字 CW；解扰节目流功能使用解密得到的控制字 CW 调用解扰算法（AES 或 CSA 算法）对节目流进行解扰，将得到的 DVB/IPTV 节目流传输给控制层；验证节目合法性功能用于提取节目流中的合法性标识水印。

[0039] 客户端的主要信息流包括：有条件接收 (CA)、有条件播出 (CP)、和盗版追踪 (PT)。，根据信息流定义，客户端函数由 CA、CP、PT 构成，分别为：

[0040]

$$\begin{cases} CA: T = DS(C, CW) \vee DS(C, K) = DS(C, \alpha D(EX(C), K) + \beta K) \\ CP: W = \begin{cases} WD(T), if(vaild=1) \\ 0, if(vaild=0) \end{cases} \\ PT: T' = FE(T, W) \end{cases}$$

[0041] 其中 DS 为解扰函数，C 为加扰或加密后的传输流，CW 为控制字生成器生成的控制字，K 为业务密钥，D 为解密函数，EX 为从传输流中解复用得到 ECM（授权控制信息）的操作

函数；WD 为合法性水印提取函数，valid 为检测是否成功的标记，valid ＝ 1 表示检测成功，载体中包含水印 W，valid ＝ 0 表示检测不成功，载体中未发现合法性水印 W；FE 为指纹水印嵌入函数，α，β ∈ {0,1} ∧ α ≠ β 。

[0042] 参见附图 3，前端子系统基本结构如下：前端子系统包括控制字生成器 (CWG)、ECM 生成器 (ECMG)、水印嵌入算法 (WEA) 和通用加扰算法 (CSA)，其主要作用是生成控制字，调用 CSA 对来自节目流管理系统的节目内容进行加扰，实现实时封装 (RP) 和预封装 (PP)。此外，为了应对非法节目的传输和干扰，在实时封装和预封装过程中通过嵌入合法性数字水印标识 W 来实现有条件播放 CP，相应的客户端子系统通过验证节目传输流中是否存在合法性水印标识 W 来实际控制节目在用户终端上的播出。

[0043] 根据信息流定义，前端子系统函数为：

[0044]

$$\begin{cases} C = PP(T) \vee RP(T) \\ \quad = S(WE(T,W),K) \vee S(WE(T,W),CW) \\ \quad = \alpha S(WE(T,W),K) + \beta S(WE(T,W)CW) \\ ECM = E(CW,K) \end{cases}$$

[0045] 其中 C 为加扰或加密后的传输流，K 为业务密钥，WE 代表合法性水印嵌入函数，S 代表加扰函数，E 代表加密函数，T 为载体，W 为合法性水印生成器生成合法性水印信息。α，β ∈ {0,1} ∧ α ≠ β

[0046] 前端子系统的控制字发生器以系统密钥为基础生成控制字，采用 DVB 通用加扰算法 (CSA) 对来自节目流管理系统（如 CDN 网络内容管理服务器）的节目内容进行加扰操作。前端子系统同时也使用会话密钥对控制字进行加密生成传统的 ECM。加扰后的节目内容与 ECM 传递给节目分发系统进行复用传输。此外，前端子系统将以固定间隔重新生成加扰控制字，保证节目内容的传输安全。在点播交互模式下，前端子系统同时也负责接收用户的播放控制信息（快进、快退、停止等），并对加扰和节目流传输进行调整。

[0047] 条件接收前端的处理过程如下：

[0048] 1) 嵌入合法性水印：为了支持条件播出和版权保护，通过水印嵌入器 WEA 的版权水印算法和合法性水印算法在 TS 传输流嵌入版权和合法性水印。版权水印比特序列由认证服务器根据前端标识和业务信息产生。合法性水印比特序列由监管机构生成。

[0049] 2) 生成 CW：对于多节目传输流和复杂的前端系统，CW 由独立加扰器生成。对于单节目传输流和低成本的前端系统，CW 由 CWG 生成。依据由 EIS（事件调度系统）提供的初始向量 (IV) 和业务标识 (AC)，CWG 通过非线性伪随机序列发生器为 TS 传输流生成 CW，并按照 5-10 秒的周期不断更新。

[0050] 3) 获取 SK：在系统运行之前，前端系统将在认证服务器中进行注册。在系统运行中，前端系统与认证服务器将建立 SAC（安全认证通道）。基于 SAC 以及业务密钥动态更新与获取协议，前端从认证服务器获取并动态更新业务密钥。

[0051] 4) 加扰和加密：加扰和加密为并行运行。嵌过版权和合法性水印的传输流 TS 送入硬件独立加扰器或者系统前端的软件加扰器进行加扰。同时，ECMG 采用 AES 算法在业务密钥 SK 的控制下对各视频业务的 CW 进行加密得到 ECM。

[0052] 前端子系统由实时封装子系统、预封装子系统、安全存储子系统构成。实时封装

子系统用于对节目内容的实时在线封装与保护，预封装子系统用于对节目内容的离线封装与保护。实时封装子系统与预封装子系统可以根据需要选择其中之一使用或者共同使用。安全存储子系统可以根据需要选择使用。在实时封装情况下，来自认证授权子系统的ski（密钥）将按照指定的时间间隔进行动态更新，采用推送方式将更新后的内容重新发送给前端子系统，前端子系统的业务密钥代理在收到推送消息后，也相应的从监听状态切换到push-ready（准备推送）状态，在检查了内部状态和存储空间后，向认证授权子系统指定的端口发送push-ready消息，激活ski的发送进程。在得到认证授权子系统的反馈，有新的sk消息到来时，业务密钥代理从监听状态切换到Recv-SKI（接收密钥）状态，解析来自认证授权子系统的消息，提取ski，存储到共享空间中。

[0053] 对于要封装的节目传输流，首先要获得其PSI/SI等传输流和业务信息，在捕获传输流中的PSI/SI数据包后，Data-process（业务加扰加密）从Read-packet（读取包信息）状态切换到Read-PSI（读取PSI）状态，从数据包中分析出PSI和SI等信息。对于预封装过程，PSI、SI信息在整个传输流中固定不变，因此只需要经历一次Read-PSI状态，对于实时封装过程，PSI、SI信息在整个传输流中可以根据运营商的要求发生改变，因此，存在PSI、SI信息更新的可能，这时需要对这些信息的版本进行识别，需要多次经历Read-PSI状态，进行相关信息的更新。

[0054] 参见图4，认证授权子系统的结构如下：认证授权子系统包括业务受理模块、业务密钥SK更新模块、双向认证协议、SK协商协议、计时器、在线用户列表等部分组成。其作用是接受用户对节目内容的申请，通过认证和协商得到业务密钥SK，并周期性的进行密钥更新。

[0055] 认证授权子系统的主要信息流包括：客户端认证(CT)、客户端授权(CR)、业务密钥更新与分配的能力(KM)，其时刻处于监听状态，对接入的客户端进行CT认证，并按照指定的时间间隔 Δ_t 动态的更新和分配业务密钥，在接收到来自客户端子系统和前端子系统子系统的业务保护信息(SPI:Service Protection Information)请求和业务授权信息(SAI:ServiceAuthorization Information)请求后，分别作出响应，执行CR授权操作。

[0056] 根据信息流定义，认证授权子系统的操作函数由CT、CR、KM构成：

[0057]
$$\begin{cases} CT: valid = I \cdot C = I(uid, h_{pass}, cert) \cdot \mathrm{C}(uid) \\ CR: p = P(uid, sid, R(uid, sid, rid, cid), key) \\ KM: KD(p, SKG(y_{n-1}, t), uid) \end{cases}$$

[0058] 其中I代表身份认证函数，C代表信用认证函数，uid为用户的身份标识，hpass为静态密码的哈希值，cert为用户身份证书，uid为用户的身份标识；R代表权利描述函数，P代表权利封装函数，sid为用户uid可以使用的业务标识，rid表示用户uid对业务sid拥有的基本权利标识，cid表示权利执行时的条件和限制；KD代表业务密钥分配函数，PKG为生成权利封装密钥的操作函数，yn为t时刻的业务密钥，$\alpha, \beta \in \{0,1\} \wedge \alpha \neq \beta$

[0059] 认证授权子系统的业务受理模块作为与用户的接口，负责根据用户的节目申请启动相应的业务流程，在用户管理系统的配合下对用户的申请及其身份信息、信用信息进行合法性和有效性验证。对于合法、有效的申请，认证授权子系统提供密钥协商机制与用户协商获得会话密钥，并将会话密钥及其相关节目信息通过安全信道发送给前端子系统系统。此外，认证授权子系统将以固定间隔重新对用户的身份进行验证和重新生成业务密钥。

[0060] 认证授权子系统的业务受理模块与客户端的业务申请模块对应进行交互，支持的业务主要包括：节目表、点播、广播等。

[0061] 在点播和广播业务下，业务受理模块从用户管理系统获得用户相关信息，通过双向认证协议确认用户的身份信息和信用信息的合法性和有效性，然后通过 SK 协商协议生成与用户端一致的业务密钥 SK，与用户信息一起发送到前端子系统，启动节目内容加扰传输过程。在成功协商密钥后，用户信息及其对应的 SK 将被保存到在线用户列表，计时器被启动。当到达指定时间间隔（该间隔规定重新认证协商的最小时间间隔，随着用户数的增多该间隔可能自动扩大）时，由 SK 更新模块对在线用户列表中的用户重新进行认证和密钥协商，更新会话密钥 SK，以提高系统的安全性。

[0062] SK 更新模块产生并定时更新业务秘钥 (SK) 以及初始向量 (IV)，并且通过 SSL（安全套接层）安全信道向记录在在线用户列表中的客户端发送 SK 更新信令，通过 TCP/IP 协议向指定 IP 和端口的前端子系统发送更新后的 SK 数据，并且保证客户端与前端子系统的 SK 数据完全一致。

[0063] 认证授权子系统与客户端的密钥更新过程如下：（点播）

[0064] 认证授权子系统与客户端建立 SSL 连接后，通过 SSL 安全信道传输用户信息；

[0065] 由用户管理系统处理用户信息，用户将点播申请表发送给认证授权子系统；

[0066] 认证授权子系统利用点播申请表的 Pid，向客户端发送相应的 SK；

[0067] 客户端接收到标志为 SK 的信息，分析该信息得到下一时刻的 SK；

[0068] 外围辅助系统

[0069] 订户管理系统提供用户注册、购买、查询服务。订户管理系统建立用户的基本信息记录，以及用户的资源信息记录，主要是智能卡相关信息的记录，并在此基础上记录用户与智能卡的对应使用情况。订户管理系统结合节目信息管理系统为用户提供订购界面，接收用户的注册、购买申请，验证用身份信息（如机顶盒编号、用户名、身份证号、公钥证书等）的合法性，生成用户注册信息库和用户订购信息库。用户可以只注册不购买，或者既注册又购买，或者不注册只购买（但必须提前注册）。节目流管理系统（如 CDN 网络内容管理服务器）对节目内容进行管理。节目信息管理系统对节目的信息进行分类，并对订户管理系统提供节目信息。

[0070] (2)DVB/IPTV 双模互动业务保护系统

[0071] 参见图 5，系统总体模块包括：业务保护 CAServer 服务器、授权管理 DRMServer 和客户端 STB 中的 CAClient 模块三部分。其中 CAServer 服务器对应前端子系统，授权管理 DRMServer 对应认证授权子系统，客户端 STB 中的 CAClient 模块对应客户端子系统。

[0072] CAServer 服务器包括接收端口、发送端口、解扰器、密钥端口四部分。1) 加扰器实现 CW（控制字）的生成，ECM（授权控制信息）的生成，TS 流的分析，ECM 的复用等加扰过程中的全部核心内容。2) 接收端口实现实时接收指定 UDP 组播地址的 TS 节目流；3) 发送端口实现实时的对加扰复用后的节目 TS 流按照指定的 UDP 组播地址转发；4) 密钥端口实现与 DRMServer 服务器的交互，并获取业务保护信息。

[0073] 授权管理 DRMServer 包括 CA 端口、STB 端口、认证与链接管理模块、节目密钥管理模块和控制模块。1)CA 端口负责接收 CAServer 服务器的业务密钥请求，并交由认证与链接管理模块建立连接后，进行业务保护信息和更新业务保护信息的传输。2)STB 端口负责

接收客户端 STB 的业务授权请求，并交由认证与链接管理模块建立安全通道后，进行业务授权信息和更新业务授权信息的传输。3) 认证与链接管理模块完成 DRMServer 服务器与 CAServer 服务器之间的链接建立与维护、完成 DRMServer 服务器与客户端 STB 之间的链接建立与维护，建立并维护安全通道。4) 节目密钥管理模块负责业务授权信息的生成、更新，负责向授权的在线客户端 STB 和 CAServer 服务器分发业务授权信息。5) 控制模块负责系统模块管理，并为多用户的并发处理提供支持，支持系统的扩展和性能提升。

[0074] CAClient 模块包括解扰器和密钥端口两部分，也可以按层次划分为控制层、业务层，业务层是核心层，实现用户的登记注册、业务授权信息获取、节目的解扰等功能。1) 解扰器实现 ECM 的解复用、TS 流的分析、CW 的解密、节目的解扰等解扰过程中的全部核心内容。2) 密钥端口实现与 DRMServer 服务器的交互，提交客户端 STB 信息，并登记用户注册信息或者获取业务授权信息。客户端 STB 通过 CAClient 模块完成对用户选择的节目进行接收、解扰、解码输出。3) 客户端 STB 根据用户操作要求，选择接入相应节目的组播地址。4) 客户端 STB 将收到的节目交给 CAClient 模块，使用业务授权信息完成对加扰控制字的解密。5) 客户端 STB 将收到的节目交给 CAClient 模块，对其进行分析、解扰；(5) 客户端 STB 将解扰后的节目进行解码输出。

[0075] (3)DVB/IPTV 双模互动业务保护系统针对不同业务模式的应用

[0076] 直播（组播）模式：

[0077] 直播（组播）系统基本工作流程：

[0078] 启动机顶盒，BOSS 系统（业务运营支撑系统）连接 CA 客户端，并浏览其所订服务列表，CA 客户端通过 EPG/Portal（电子节目指南 / 门户技术）向 BOSS 提供客户端 ID 和服务列表，订购节目或请求节目播放；

[0079] CA 客户端向授权服务器提供客户端 ID，并发送服务授权信息请求；授权服务器通过查找在线用户信息，并与 BOSS 间进行客户端 ID 的认证，生成服务授权信息，BOSS 的资产管理模块确认用户的账户能否满足所订节目所需，若能满足，BOSS 向授权服务器返回服务授权信息的请求结果；

[0080] 若通过授权，传递指令给流服务器，节目数据流 TS 根据请求的服务列表由 SS（流服务器）发出，通过 CA 服务器，CA 服务器向授权服务器发送服务保护信息请求；授权服务器给服务列表生成相应的系统密钥信息和服务保护信息，并返回 CA 服务器服务保护信息的请求结果；

[0081] 在 CA 服务器端，TS 流经过 PSI（节目设定信息）分析、加扰、加密，传送给 CA 客户端；CA 客户端经过与 CA 服务器端相反的处理，解扰解密 TS 后并传送到屏幕显示。

[0082] 授权服务器通过推送接口分别向 CA 服务器和 CA 客户端的授权控制信息接口推送服务保护信息，用来加扰和解扰。

[0083] 点播模式：

[0084] 点播 iCAS 系统基本工作流程：

[0085] 启动机顶盒，BOSS 系统连接 CA 客户端，并浏览其所订服务列表，CA 客户端通过 EPG/Portal 向 BOSS 提供客户端 ID 和媒体列表，订购节目或请求节目播放；

[0086] CA 客户端向授权服务器提供客户端 ID，并发送媒体授权信息请求；授权服务器通过查找在线用户信息，并与 BOSS 间进行客户端 ID 的认证，生成媒体授权信息，BOSS 的资产

管理模块确认用户的账户能否满足所订节目所需，若能满足，BOSS 向授权服务器返回媒体授权信息的请求结果；

[0087] 若通过授权，传递指令给 VOD 服务器，节目数据流 TS 根据请求的媒体列表由 VS（视频点播服务器）发出；

[0088] 预封装服务器向授权服务器发送媒体保护信息请求；授权服务器给媒体列表生成相应的系统密钥信息和服务保护信息，并返回预封装服务器媒体保护信息的请求结果；

[0089] 在预封装服务器，TS 流根据 C/S 或 B/S 工作方式的预封装协议（预封装协议：BOSS 系统中的资产管理向预封装服务器发送原始的 URL 和加密后的 URL，并对加扰深度及加扰模式等配置，预封装服务器将结果返回。）进行 PSI 分析、加扰、加密后，传送给 VOD 服务器；CA 客户端通过访问 Web 页面获得所需内容，经过与预封装服务器端相反的处理，解扰解密 TS 后并传送到屏幕显示。

[0090] 授权服务器通过推送接口分别向预处理服务器和 CA 客户端的授权控制信息接口推送媒体保护信息，用来加扰和解扰。

[0091] (4) 加密模式可控的信息流加密传输

[0092] 该系统在前端子系统的预封装模块中加扰模块采用 CSA 和 AES 两种算法，可根据环境需要实时改变加扰算法。加密模块采用 AES 算法对 CW 加密，支持 CBC（反向块链接模式）、OFB（输出反馈模式）、CFB（密码反馈模式）、CTR（技术模式）、ECB（电子密码本模式）五种加密模式对授权控制信息 ECM 进行加密，可在前端子系统配置参数结构体中可以任意选取，从而实现了信息流的保密传输。具体流程如下所示。

[0093] 1)chi 为需要保护传输的节目流，可以是单一逻辑频道，也可以是单一物理频道；

[0094] 2)ski 为与节目（组）chi 相关的业务密钥，由认证授权子系统控制产生和更新；

[0095] 3)P 为所有 ski 构成的集合，Q 为用户所选择 chi 对应的 ski 构成的子集，并加密传输给用户；

[0096] 4)cwit 为在 t 时刻加扰 chi 时使用的控制字，长度为 64bits(CSA) 或 128bits(AES)；

[0097] 5)S(·) 为对 tsi 的加扰函数，可选择为 CSA 和 AES，加扰密钥为 cwit（注：S(·) 和 S-1(·) 选择算法和密钥应一致）；

[0098] 6)S-1(·) 为对 tsi 的解扰函数，可选择为 CSA 和 AES，加扰密钥为 cwit（注：S(·) 和 S-1(·) 选择算法和密钥应一致）；

[0099] 7)ECMi 为与 chi 对应的授权控制信息，包含 cwit 及其相关信息；

[0100] 8)E(·) 为 ECMi 生成函数，选择为 AES，加密模式为 CBC、CFB、OFB、CTR 之一，加密密钥为 ski（注：D(·) 和 E(·) 选择算法和模式、密钥应一致）；

[0101] 9)D(·) 为 ECMi 解密函数，选择为 AES，加密模式为 CBC、CFB、OFB、CTR 之一，解密密钥为 ski（注：D(·) 和 E(·) 选择算法和模式、密钥应一致）。

[0102] (5) 简化的业务保护层次

[0103] 该系统采用双层加密策略，包含两个加密层次，即单节目相关层 (PRL：Program Related Layer) 和业务相关层 (SRL：Service Related Layer)。PRL 层实施基于控制字 cw 对视频内容的加扰，SRL 层基于业务密钥通过加密生成业务相关控制信息 (SRI：Service Related Information)，即授权控制信息 ECM。加扰以 CW 为密钥，调用通用加扰算法 CSA 完

成对欲传输节目内容的直接加扰保护。加密以业务密钥 SK 为密钥，调用加密算法，如 AES，实现对控制字 CW 的加密，形成授权控制信息 (ECM)。CW 保证节目内容的安全传输，同时 CW 与 SK 的分离，也使得节目内容的加扰与用户无关，降低了系统的复杂性。

[0104] 授权控制信息 ECM 进一步与加扰后的节目流复用形成传输流，通过复用信道分发给客户端。由于 ECM 与用户相关，因此只有持有 SK 的用户才能解扰，实现有条件接收的目标。对于终端消费者，如果需要访问某个视频业务，必须通过 IP 双向通道与认证服务器交互获得与消费者相关的授权管理信息。

[0105] 在 PRL 层，视频业务传输流在加扰密钥 CW 的控制下加扰。CW 由前端的 CW 生成器 (CWG) 生成，加扰算法采用通用加扰算法 (CSA) 以便与 DVB-CAS 兼容。在 SRL 层，CW 将在业务密钥 SK 的控制下加密生成 ECM。而业务密钥 SK 则是由认证授权子系统与客户端的业务申请模块通过密钥协商协议产生。ECM 将被复用到加扰后的传输流中。在消费者机顶盒等终端中完成相反的过程，解复用 ECM 并解密恢复出 CW，进而得到原始的传输流送给解码器。与前端相同，客户端也将从认证授权子系统获取和动态更新业务密钥 sk。

[0106] (6) 业务密钥更新

[0107] 该系统运用了动态密钥更新与分配技术。动态密钥更新与分配分为两个阶段，分别是业务密钥交换阶段和动态业务密钥推送阶段。认证授权子系统与客户端的业务申请模块通过密钥协商协议产生业务密钥 SK。在成功协商密钥后，用户信息及其对应的 SK 将被保存到在线用户列表，计时器被启动。当到达指定时间间隔（该间隔规定重新认证协商的最小时间间隔，随着用户数的增多该间隔可能自动扩大）时，由 SK 更新模块对在线用户列表中的用户重新进行认证和密钥协商，更新会话密钥 SK，以提高系统的安全性。其中，业务密钥 SK 采用 SSL 等方式通过安全信道进行分发。除业务密钥 SK 外，本系统中还包含控制字 CW 和系统密钥 MK。其中控制字 CW 的更新与用户无关，按指定间隔（如 10seconds）进行更新。当发现业务运营出现问题时，系统密钥才进行更新，或者当到达指定时间间隔（如 1month）时进行更新。

[0108] 系统在更新业务密钥的过程中，分别采用了密钥分级更新技术和经过改进的组密钥更新技术。所谓密钥分级更新，就是 DRM 授权认证系统在进行密钥更新时，上一级 DRM Server 只对本区内的 DRM Server 进行密钥更新，而不直接对用户提供服务，而改进的组密钥协议的特点是考虑到电视业务的具体业务特点，将广播业务和其他增值业务进行区别对待，如果用户已经订购了指定的广播业务，那么在切换使用其他业务时，DRM 系统不对广播业务密钥更新，只对增值业务进行密钥更新处理，而且在密钥更新的过程中寻找组密钥更新的最少节点，进一步降低业务密钥更新的通信开销和计算能力损耗。

[0109] 认证授权子系统与前端子系统的密钥更新过程如下：认证授权子系统与前端子系统建立 TCP/IP 连接，打开前端子系统的网络监听，实时对认证授权子系统发送的消息进行分析；认证授权子系统在规定的时间间隔发送更新的 SK 信息；前端子系统接收到认证授权子系统发送的消息标志为 SK 的信息后，对该信息进行分析。对当前的 SK 进行验证并提取出下一个时刻使用的 SK 数据。然后向认证授权子系统发送确认信息。完成认证授权子系统与前端子系统的密钥更新。

[0110] 认证授权子系统与客户端的密钥更新过程（广播）如下：认证授权子系统与客户端建立 SSL 连接后，通过 SSL 安全信道传输用户信息；认证授权子系统根据在线用户列表获

得用户节目 Pid 和用户信息后，通知 SSL 是否传输给用户业务密钥，以及其节目 Pid ；客户端接收到标志为 SK 的信息，保存备用。

[0111] 认证授权子系统与客户端的密钥更新过程（点播）如下：认证授权子系统与客户端建立 SSL 连接后，通过 SSL 安全信道传输用户信息；由用户管理系统处理用户信息，用户将点播申请表发送给认证授权子系统；认证授权子系统利用点播申请表的 Pid，向客户端发送相应的 SK ；客户端接收到标志为 SK 的信息，分析该信息得到下一时刻的 SK。

[0112] (7) 基于代理的预封装技术

[0113] 参考图 6，该系统模型采用 C/S 结构，如图所示。右面的预封装系统端是服务器，视频输入是客户端。在预封装系统内部亦使用 C/S 模式，由主服务器和代理服务器组成，代理服务器对主服务器来说是服务器端，主服务器是客户端。

[0114] 整个模型的设计思想为：对需要封装加密的视频，首先进入主服务器，其根据视频大小进行判断，选择是否需要代理服务器封装。若不需代理执行，则不分割视频文件，自己直接进行封装加密；若需要代理执行，则将视频文件根据设计的算法均分为几小段，然后自动搜索网络上的空闲代理服务器，将已分段的视频传送给可用的代理，让其执行封装功能。代理服务器封装完成之后，再及时返回给主服务器端，由主服务器端将返回的分段进行重组，恢复成一个完整的已封装好的“原视频”文件。

[0115] 代理服务器主要包括预封装主控模块和预封装代理模块。根据预封装主控模块的功能可将其分为两部分：一部分是中央控制器，主要实现对视频文件的代理封装操作，如分割、调度与合并；另一部分是独立预封装模块，即不使用代理服务器，直接对视频内容完成封装功能。

[0116] 基于代理的预封装技术方法主要包括视频分割，视频调度和密钥获取。

[0117] 视频分割对于需要封装的视频来说，设其大小为 m(mb)，需分割段数为 s，视频封装速度为 k(mb/s)，视频传输的速度为 v(mb/s)，视频分割需要时长 t1，视频合并所耗时长为 t2。在具体执行过程中，按如下规则进行：分割一段，传输一段；传输的同时，要进行实时的封装；视频段封装完成后立刻传回去；传回几段，则合并几段。应该分割的段数 s 应该满足公式：$\Delta t_1+\Delta t_2 \cdot s+2(m/s)/v+(m/s)/k < m/k$，其中，m/k 为独立预封装所需要的时间。

[0118] TS 视频文件是由多个 188 字节的 TS 包组成，因此分割视频的大小和分割视频件时所需要的缓冲区大小均应为 188 字节的整数倍。设输入的视频大小为 n 万个 TS 包，分割思想为：

[0119] (1)n <= 160 时，视频不分割；

[0120] (2)160 < n <= 320 时，视频分割为 2 段；

[0121] (3)320 < n <= 480 时，视频分割为 3 段；

[0122] (4)480 < n <= 640 时，视频分割为 4 段；

[0123] (5)n > 640 时，视频分割为 5 段。

[0124] 视频调度主要实现了主控模块选择代理模块使之完成预封装的过程，具体流程为：预封装主控模块启动之后定时发送广播消息，在线的预封装代理模块收到广播消息后，向预封装主控模块端发送确认信息，预封装主控模块将各预封装代理模块的情况保存到数据库中。预封装主控模块端请求代理后，便开始传输视频，视频传送的相关信息会被保存到对应的日志文件（包括视频名称、视频传送时间、视频被传到的代理标识等）中。当视频

分段数少于回应的代理数时，需要随机选择其中的几个代理执行封装过程，具体过程为：1）将收到的代理的标识映射为 1-100 之间的整数（假设代理总数＜＝ 100）；2）根据视频的分割数量，确定需要的代理数 n；3）使用伪随机数发生器产生 1-100 之间的 n 个数；4）根据产生的随机数找到对应的代理标识，最终确定需要的封装代理。

[0125] 密钥获取包括前端子系统子系统预封装服务密钥的获取和客户端子系统预封装密钥获取。前端子系统子系统预封装服务密钥的获取流程为：视频内容 DBMS（数据库管理服务器）根据 Mlist（媒体列表）向预封装主控模块发送传输流，预封装主控模块给认证授权子系统的认证授权模块发送一个 MPI（媒体保护信息）请求；认证授权模块建立 MKI（媒体密钥信息），生成 MPI，将 MKI 存储到数据库，并以 Mlist 为索引；认证授权模块返回给预封装主控模块 MPI 请求结果；预封装主控模在调用代理完成预封装后，将 TS 传送回给 DBMS。客户端子系统预封装密钥获取流程为：启动机顶盒后，客户端接收到来自视频服务器的已封装好的视频内容；客户端子系统向认证授权子系统的认证授权模块提供客户端标识和从视频传输流中获取的媒体列表 Mlist，发送 MAI 请求；认证授权模块与订户管理模块间进行客户端标识的认证，订户管理模块向认证授权模块返回可以为用户授权的媒体列表 Mlist'，根据数据库中的 Mlist' 信息生成 MAI；认证授权模块返回给客户端子系统 MAI 请求结果；客户端子系统即可解扰并收看视频内容。

[0126] 该系统支持离线数据处理，当预封装系统服务器需要关闭或者中断服务时，可以先通过中央控制器，选择代理服务器，在视频传送之后，即关闭或中断服务。当预封装系统服务器的服务再次开启后，代理端会自动将视频发过来，服务器只需进行以后的操作就可以了。另外，还可以减轻主服务器负担，实现高效率封装。当一路视频需要封装时，若使用代理服务器帮忙，处理时间会减少；多路视频需要加扰时，服务器端由于运算能力的限制，要完成多数据量的加扰工作，会给服务器带来过大的负担，影响封装的效率。而如果将多个视频数据进行处理，然后交给代理服务器进行封装的工作，这样会加快封装的效率，减轻服务器端的负担。代理服务器的数量决定了视频分段的多少，代理服务器越多，视频的分段数越多。视频分的段数越多，就会使每个视频段所包含的数据量减少，这样一方面可以进一步减少传输时间，另一方面，所有代理服务器上的封装视频段所需时间也会变少，从而在整体上提高了工作效率。

[0127] 分布式预封装系统，若在高性能的网络环境下，将更具有优势。视频文件的传输可以借助于高带宽网络或光纤等更加快速的传输介质，将视频文件进行实时的发送与接收。由于光纤等传输介质的传输速度非常快，在多个视频分段传输方面，不会占用太长时间，因而整个系统的效率会提高。

[0128] （8）安全存储

[0129] 该系统基于随机过程的存储空间遍历算法实现了安全存储。该系统设计了密钥分发中心（Key Distribution Center，KDC）来为客户端的加解密文件提供业务密钥，KDC 先获得客户端密文文件的分割情况（例如 n 个子文件），生成相应的 1 至 n 不重复的随机序列，客户端根据随机序列依次向存储服务器发送密文子文件；存储服务器建立新文件，将收到的密文子文件写入新文件，直至密文子文件发送完毕；这样，存储服务器中便存入了乱序的密文文件，文件上传成功。当用户申请下载文件时，存储服务器获取文件路径，查找到文件，将乱序的密文文件直接发送客户端，直接在客户端完成数据的安全解密，保护文件端到

端的加密传输和数据的安全存储。

[0130] (9) 选择性加扰深度控制

[0131] 该系统为了实现对加扰深度更加精确的控制，对 I 帧和 I- 宏块的计数方法采用新的双上限计数 (n1，n2) 的方法，使得计数上限 n 值都可用和任意加扰深度 d 都可以选择。对任意的 d，如果 ：1)1/d 为整数，则令 n1 ＝ 1/d，n2 ＝ 1 ；2)1/d 不是整数，则将 d 表示为分式，并用欧几里德算法得到分子分母的最大公约数 r，约后得 d ＝ a/b，令 ：$\begin{cases} n1 = \lfloor b/a \rfloor \\ n2 = b \end{cases}$ 。

[0132] 对找到的 I 帧计数 c1，c2，当 c1 达到上限 n1 时，对当前帧执行加扰操作 ；当 c2 达到上限 n2 时，两个计数器都清零，c1 ＝ c2 ＝ 0。

[0133] 在实际应用中提供两种加扰深度的设置方式 ：1)n 方式设置，n 为加扰上限，实际设置加扰深度为 1/n ；2)d 方式设置，d 为加扰深度，加扰上限 n 值采用上述的双上限计数方法确定。

[0134] (10) 密钥更新批处理策略

[0135] 系统设计引入密钥更新批处理策略，提供百万用户规模的密钥实时更新与分配，降低了系统开销，增强了整个密钥更新的能力，提升了系统的安全性，为付费电视业务提供了灵活多变的保护机制。提出的这种密钥管理结构包括一个授权服务器 (AS，Authentication Server) 和多个密钥服务器 (KS，Key Server) 这两个主要部分。授权服务器作为树根，分发业务保护的关键信息，并通过密钥服务器管理间接管理所有用户。

[0136] 授权服务器，它包括用户认证模块、密钥服务器模块以及用户授权模块。其作用包括通过 SSL 安全信道接收用户的接入 (离开) 请求，并对用户进行身份认证 ；如果发生授权组成员变更，授权中心的密钥服务器管理模块通过 SSL 安全信道获取各个密钥服务器模块产生的点播业务密钥并通过单向函数计算出广播业务密钥，同时通知点播业务密钥服务器更新其子授权组广播 (点播) 业务密钥，承担授权服务器与各个点播密钥服务器构成的密钥树的建立和维护工作 ；授权系统通过 ES(Encryption System) 接口与前端加扰服务器进行控制字加扰密钥信息交互，从而将各个密钥服务器的组播密钥作为控制字加扰密钥发送给加扰服务器 ；授权服务器与用户管理系统进行用户信息的交互，由授权中心签发基于 x.509 标准的数字证书。该证书用于授权用户在申请加入授权组时进行身份认证。

[0137] 密钥服务器，包括密钥生成模块、密钥分发模块以及密钥管理模块。其功能包括通过密钥生成模块产生伪随机数，作为待分发的点播业务密钥 ；由密钥分发模块实现针对授权组成员的组密钥分发 ；密钥管理模块与授权服务器进行数据交互，在授权服务器发出添加 (删除) 指定成员的指令时，密钥管理模块通知密钥生成模块产生新的点播业务密钥，然后密钥管理模块将经过更新后的点播密钥发送给授权服务器，并由密钥分发模块对指定的用户密钥节点进行密钥更新。

[0138] 参见图 7，假定 u3 和 u4 是两个申请转移子授权组的用户。u3 从 A 组转移到 B 组，u4 从 B 组转移到 A 组。u4 替换了 u3 原来的位置，u3 替换了原来 u4 的位置。需要更新的密钥节点为 K_A 和 K_B。要确定密钥更新路径，只需在每次更新的过程中，我们跟踪每个需要更新密钥的节点，对其上一级需要更新密钥的节点进行标记。在这个过程中，如果发现有一个节点被标记两次则停止该路径的标记。直到所有路径标记完毕，密钥更新路径就确定了。在整个密钥树中，只有 K_A' 和 K_B' 需要更新。K_A 点播业务密钥更新为 K_A'，K_B 点播业务密钥

更新为 K_B'。点播业务密钥服务器 A 向 u1 发送，向 u2 发送，向 u4 发送。点播业务密钥服务器 B 向 u3 发送，向 u5 发送，向 u6 发送。

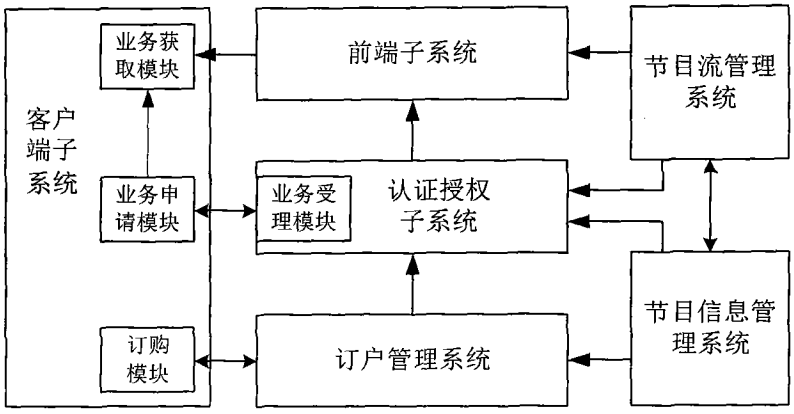

客户端子系统
业务获取模块
业务申请模块
订购模块
前端子系统
业务受理模块
认证授权子系统
订户管理系统
节目流管理系统
节目信息管理系统

图 1

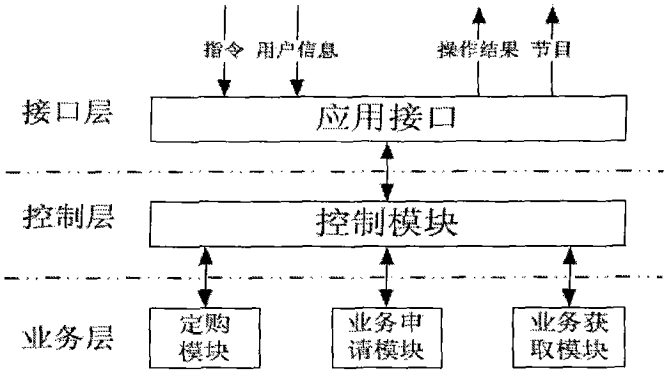

指令
用户信息
操作结果
节目
接口层
应用接口
控制层
控制模块
业务层
定购模块
业务申请模块
业务获取模块

图 2

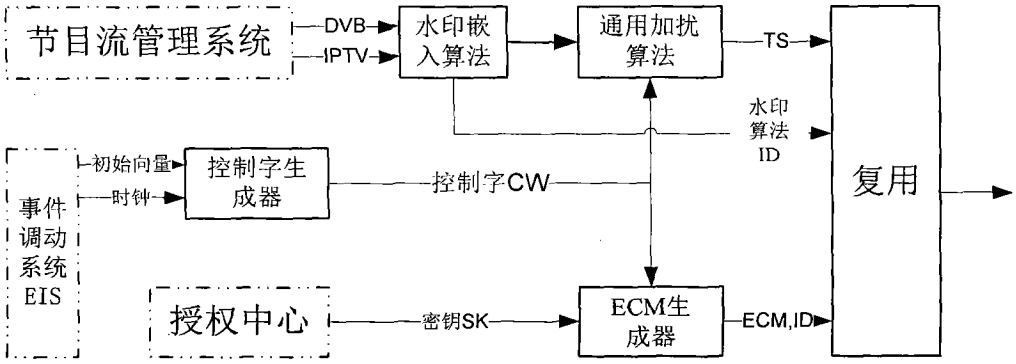

节目流管理系统
DVB
IPTV
水印嵌入算法
通用加扰算法
TS
水印算法ID
复用
初始向量
时钟
控制字生成器
控制字CW
事件调动系统EIS
授权中心
密钥SK
ECM生成器
ECM,ID

图 3

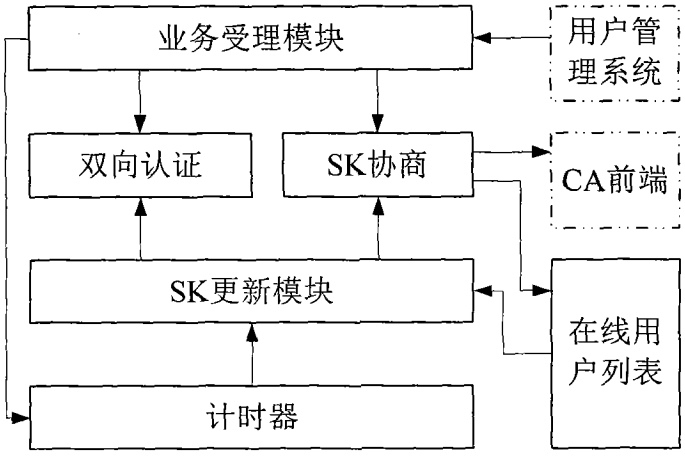

业务受理模块
用户管理系统
双向认证
SK协商
CA前端
SK更新模块
在线用户列表
计时器

图 4

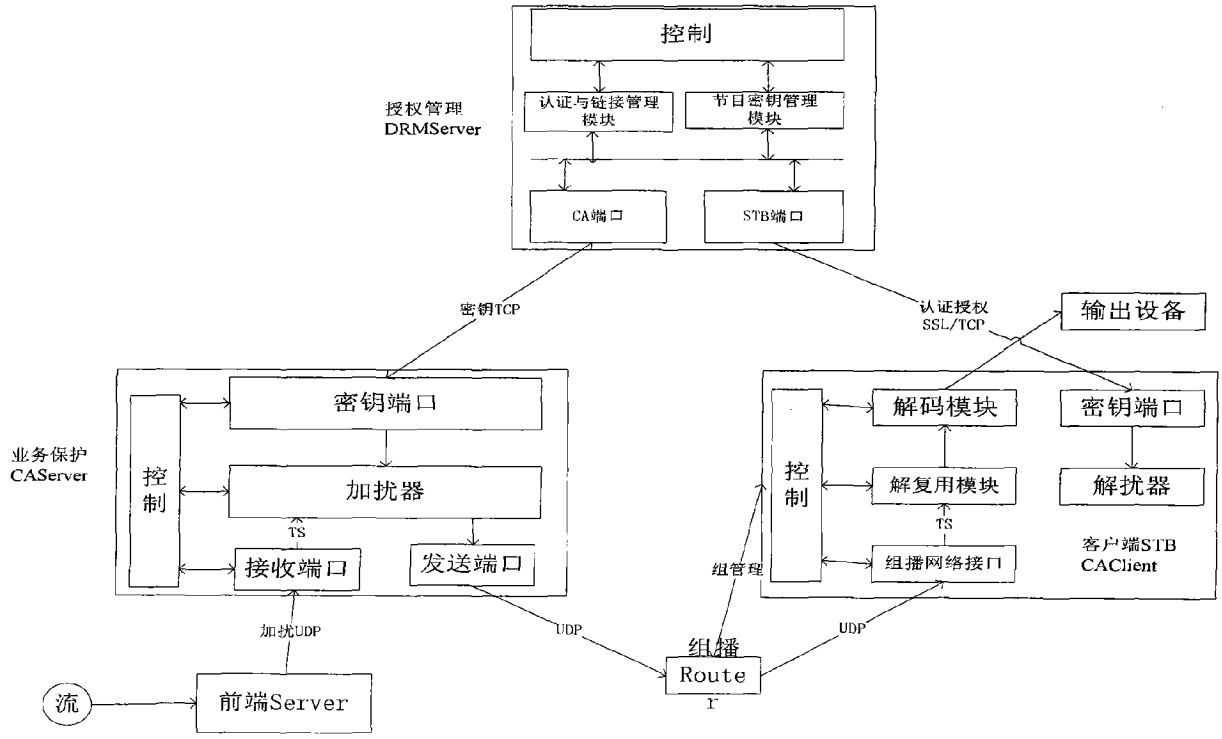

控制
授权管理
DRMServer
认证与链接管理模块
节目密钥管理模块
CA端口
STB端口
密钥TCP
认证授权
SSL/TCP
输出设备
业务保护
CAServer
控制
密钥端口
加扰器
TS
接收端口
发送端口
加扰UDP
UDP
组播
Route
r
流
前端Server
组管理
控制
解码模块
密钥端口
解复用模块
解扰器
TS
组播网络接口
客户端STB
CAClient
UDP

图 5

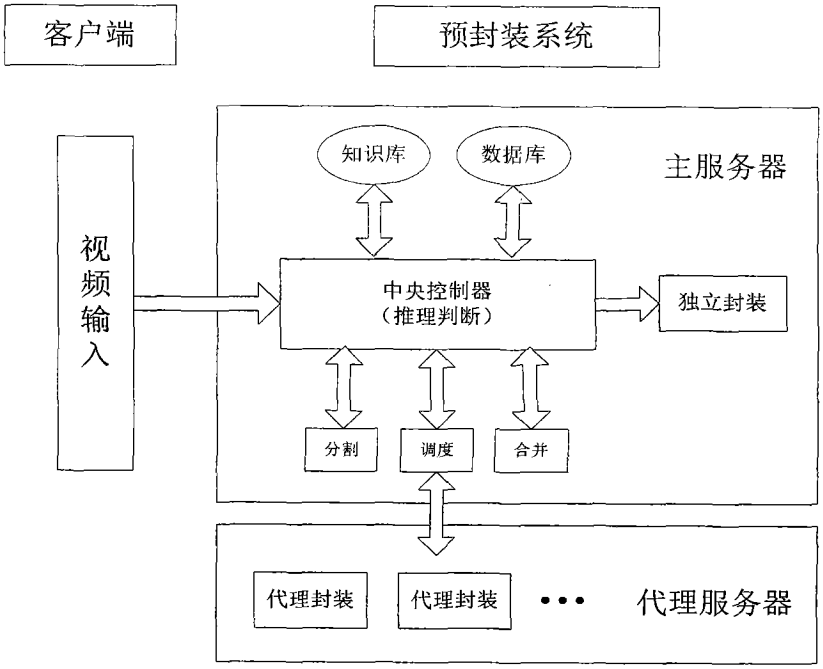

客户端
预封装系统
视频输入
知识库
数据库
主服务器
中央控制器
（推理判断）
独立封装
分割
调度
合并
代理封装
代理封装
代理服务器

图 6

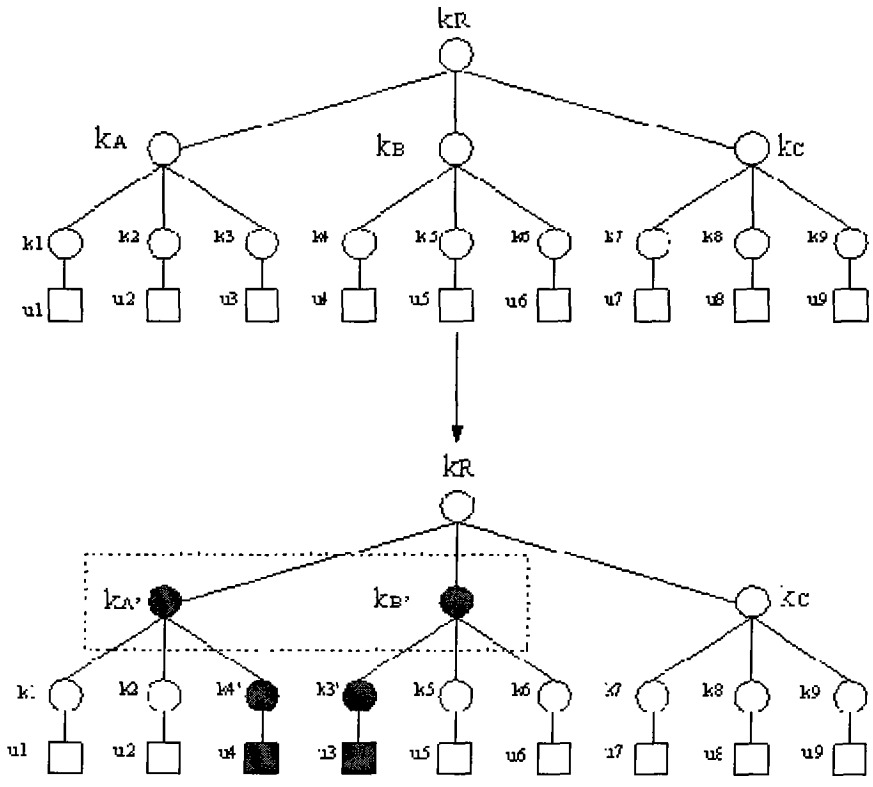

kR
kA
kB
kC
k1
k2
k3
k4
k5
k6
k7
k8
k9
u1
u2
u3
u4
u5
u6
u7
u8
u9

图 7