

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200510105477.7

[43] 公开日 2006 年 11 月 15 日

[11] 公开号 CN 1863041A

[22] 申请日 2005.9.28

[21] 申请号 200510105477.7

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

[72] 发明人 孙 超

[74] 专利代理机构 北京凯特来知识产权代理有限公司
代理人 郑立明

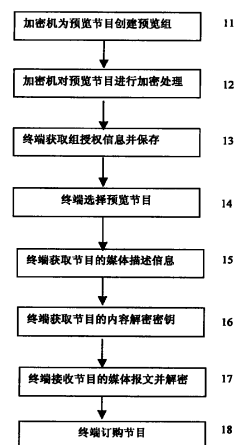
权利要求书 3 页 说明书 11 页 附图 1 页

[54] 发明名称

实现网络电视节目预览的方法

[57] 摘要

本发明公开了一种实现网络电视 IPTV 节目预览的方法，该方法的核心为：在开放移动联盟数字版权管理 OMA DRM 加密系统中，建立预览组；OMA DRM 根据预览组为终端生成组授权信息，并下发至终端；终端根据其接收的组授权信息，获取其从对应预览组中选择的各预览节目的内容加密密钥 CEK 或生成 CEK 的种子，并对其选择的各预览节目进行解密，实现 IPTV 节目的预览。采用本发明所述的方法，能够实现对批量节目进行预先授权，不但可以减少对版权中心的并发访问量，提高系统的可靠性；而且可以减少用户等待时间，提高用户的体验；另外，可配置的预览规则为运营商提供了灵活的业务运营的方法，比如可以将预览规则相同的多个节目进行打包发售。



1、一种实现网络电视IPTV节目预览的方法，其特征在于，包括：

A、在开放移动联盟数字版权管理OMA DRM加密系统中，建立预览组；

B、OMA DRM根据预览组为终端生成组授权信息，并下发至终端；

C、终端根据其接收的组授权信息，获取其从对应预览组中选择的各预览节目的内容加密密钥CEK或生成CEK的种子，并对其选择的各预览节目进行解密，实现IPTV节目的预览。

2、根据权利要求1所述的方法，其特征在于：所述步骤A具体包括：

A1、加密机根据预览规则为预览节目创建预览组，并确定预览组的组加密密钥GEK；

A2、加密机将GEK作为加密密钥对预览组的各预览节目的CEK或生成CEK的种子进行加密；

A3、将加密后信息承载在预览节目的媒体描述信息或媒体报文中。

3、根据权利要求2所述的方法，其特征在于：对所述预览组的各预览节目的CEK或生成CEK的种子进行加密的加密算法为对称加密算法，所述预览组的各预览节目的CEK或生成CEK的种子解密密钥为所述预览组的GEK。

4、根据权利要求2所述的方法，其特征在于，所述步骤A3具体包括：

将所述各预览节目的CEK或生成CEK的种子进行加密后的信息承载于预览节目的媒体描述信息的国际流媒体联盟加密键ISMACrypKey中的内容密钥Content Key参数中，或者，承载于预览节目的媒体报文的附加段中。

5、根据权利要求4所述的方法，其特征在于，所述步骤A还包括：

加密机将各预览节目对应的预览组的Group ID信息承载于各预览节目的

媒体描述信息的国际流媒体联盟加密键ISMACrypKey中的Group ID参数中。

6、根据权利要求5所述的方法，其特征在于，所述步骤B具体包括：

终端完成到版权中心的注册时，根据电子节目指南EPG的通知，向版权中心申请下发自身没有保存过的预览组的组授权信息，版权中心生成相应的组授权信息并下发至终端，终端进行保存；或者，

终端在选择预览节目后，当该节目所在预览组的组授权信息不存在时，根据该节目所在预览组Group ID向版权中心申请下发相应的组授权信息，版权中心生成相应的组授权信息并下至终端，终端进行保存。

7、根据权利要求6所述的方法，其特征在于，步骤B中所述组授权信息包括：

相应预览组的Group ID、预览规则、预览节目的CEK或生成CEK的种子的解密密钥以及解密算法信息。

8、根据权利要求7所述的方法，其特征在于，所述步骤C具体包括：

C1、终端选择预览组中的预览节目后，根据接收到的媒体服务器下发的其选择的预览节目的媒体描述信息的加密键ISMACrypKey中的Group ID参数所承载的Group ID信息确定保存在终端中的相应的组授权信息，并获取该预览节目的CEK或生成CEK的种子的解密密钥和解密算法信息；

C2、终端根据获取的所述预览节目的CEK或生成CEK的种子的解密密钥和解密算法信息解密所述预览节目的ISMACrypKey中Content Key参数或者所述预览节目的媒体报文的附加段中的信息，获取所述预览节目的CEK或生成CEK的种子；

C3、终端中的数字版权管理代理DRM Agent根据获取的所述预览节目的CEK或生成CEK的种子解密各预览节目的媒体报文，实现IPTV节目的预览。

9、根据权利要求8所述的方法，其特征在于，该方法还包括：

加密机在对预览节目的内容进行加密时，该预览节目的媒体报文生成附加段，并在所述附加段中根据该预览节目的预览规则设置该预览节目当前所处阶段的标识；且所述步骤C3具体包括：

终端中的DRM Agent根据所述的阶段标识和所述预览节目的CEK或生成CEK的种子解密各预览节目的媒体报文，实现IPTV节目的预览。

10、根据权利要求9所述的方法，其特征在于，所述步骤C3具体包括：

终端中的DRM Agent 确认所述阶段标识为可预览阶段的标识后，根据获取的所述预览节目的CEK或生成CEK的种子解密各预览节目的媒体报文，实现IPTV节目的预览；或者，

当终端中的DRM Agent 确认所述预览节目的媒体报文附加段中所承载的阶段标识为不可预览阶段的标识后，终端根据所述节目的内容标识Content ID进行节目订购处理。

实现网络电视节目预览的方法

技术领域

本发明涉及网络通信技术领域，尤其涉及一种实现网络电视节目预览的方法。

背景技术

流媒体进行传输时所涉及的主要协议包括RTP（Real-Time Transport Protocol，实时传送协议）、RTSP（Real-Time Streaming Protocol，实时流协议）、SDP（Session Description Protocol，会话描述协议）等。各协议的主要功能如下：

RTP协议：用于承载音频、视频数据；RTP流的加密采用ISMA（Internet Streaming Media Alliance，国际流媒体联盟）加密规范。

RTSP协议：用于建立到媒体服务器的会话连接，也用于指示用户的播放操作，如播放、暂停、快进、快退等操作。

SDP协议：用于描述节目的会话数据，如媒体类型、速率、带宽、媒体服务器IP地址、端口等；当编码器制作流媒体节目时，都会产生一个相应的SDP文件，用于描述上述信息。

在目前的IPTV（网络电视）业务提供过程中，一般由MDN（Media Distribute Network，媒体分发网络）实现节目的预览功能。该方法是通过抽取节目中的片断组成新的节目，通过用户的点播实现该节目的预览。

但是该技术方案存在以下缺点：

1、无法实现对加密节目的预览，因为MDN抽取片断实现预览的方式需要先有不加密的节目，通过对不加密节目抽取片断形成新的媒体文件，因此无法保证节目的安全性；

2、如果预览部分的节目有加密需求，则还要将抽取的片断通过加密机再次加密，处理流程复杂。

随着流媒体在互联网上的广泛传播又发展起来一种新技术DRM（Digital Right Management，数字版权管理），利用DRM不仅可以实现对数字内容的保护，同时还可以提供节目预览、批量订购等业务部署功能。

因此，随着DRM技术的出现，又出现了一种实现IPTV节目预览的方法，该方法是基于OMA（Open Mobile Alliance，开放移动联盟）DRM的加密系统，通过对终端进行预览授权来实现的。

具体方法是：将预览节目进行一级加密，并将节目的内容加密密钥承载在预览版权中，该预览版权中还承载有允许预览的时间、次数以及有效期等信息；当终端提出预览申请，在版权中心完成注册后，版权中心根据用户的申请，将相应预览节目的版权下发给终端，终端通过版权获取节目的内容密钥对节目内容进行解密后，播放节目供用户预览；当节目的播放时间达到预览版权中规定的预览时间后，预览版权失效，从而实现对节目预览的目的。

上述技术方案虽然能够实现对加密节目的预览，而且也省去了再次加密的流程，但是，不难看出，该技术方案存在如下缺点：

1、极大地增加了版权中心的并发访问量，降低了系统的可靠性。因为预览功能一般对用户是免费的，用户通常的操作习惯是在大量的节目间通过预览选择一个最终决定付费观看的节目，而每次的预览操作都需要从版权中心申请下发一个预览版权，因此当大量用户选择节目时必然对版权中心的性能提出较高的要求；

2、由于每次预览一个节目都需要有申请预览版权的过程，导致用户等待

时间长、体验差。

发明内容

鉴于上述现有技术所存在的问题，本发明的目的是提供一种实现IPTV节目预览的方法，实现对批量节目进行预先授权，减少对版权中心的并发访问量，提高系统的可靠性。

本发明的目的是通过以下技术方案实现的：

本发明提供了一种实现网络电视IPTV节目预览的方法，包括：

- A、在开放移动联盟数字版权管理OMA DRM加密系统中，建立预览组；
- B、OMA DRM根据预览组为终端生成组授权信息，并下发至终端；
- C、终端根据其接收的组授权信息，获取其从对应预览组中选择的各预览节目的内容加密密钥CEK或生成CEK的种子，并对其选择的各预览节目进行解密，实现IPTV节目的预览。

所述步骤A具体包括：

- A1、加密机根据预览规则为预览节目创建预览组，并确定预览组的组加密密钥GEK；
- A2、加密机将GEK作为加密密钥对预览组的各预览节目的CEK或生成CEK的种子进行加密；
- A3、将加密后信息承载在预览节目的媒体描述信息或媒体报文中。

其中，对所述预览组的各预览节目的CEK或生成CEK的种子进行加密的加密算法为对称加密算法，所述预览组的各预览节目的CEK或生成CEK的种子解密密钥为所述预览组的GEK。

所述步骤A3具体包括：

将所述各预览节目的CEK或生成CEK的种子进行加密后的信息承载于预览节目的媒体描述信息的国际流媒体联盟加密键ISMACrypKey中的内容密钥Content Key参数中，或者，承载于预览节目的媒体报文的附加段中。

所述步骤A还包括：

加密机将各预览节目对应的预览组的Group ID信息承载于各预览节目的媒体描述信息的国际流媒体联盟加密键ISMACrypKey中的Group ID参数中。

所述步骤B具体包括：

终端完成到版权中心的注册时，根据电子节目指南EPG的通知，向版权中心申请下发自身没有保存过的预览组的组授权信息，版权中心生成相应的组授权信息并下发至终端，终端进行保存；或者，

终端在选择预览节目后，当该节目所在预览组的组授权信息不存在时，根据该节目所在预览组Group ID向版权中心申请下发相应的组授权信息，版权中心生成相应的组授权信息并下至终端，终端进行保存。

步骤B中所述组授权信息包括：

相应预览组的Group ID、预览规则、预览节目的CEK或生成CEK的种子的解密密钥以及解密算法信息。

所述步骤C具体包括：

C1、终端选择预览组中的预览节目后，根据接收到的媒体服务器下发的其选择的预览节目的媒体描述信息的加密键ISMACrypKey中的Group ID参数所承载的Group ID信息确定保存在终端中的相应的组授权信息，并获取该预览节目的CEK或生成CEK的种子的解密密钥和解密算法信息；

C2、终端根据获取的所述预览节目的CEK或生成CEK的种子的解密密钥和解密算法信息解密所述预览节目的ISMACrypKey中Content Key参数或者

所述预览节目的媒体报文的附加段中的信息，获取所述预览节目的CEK或生成CEK的种子；

C3、终端中的数字版权管理代理DRM Agent根据获取的所述预览节目的CEK或生成CEK的种子解密各预览节目的媒体报文，实现IPTV节目的预览。

该方法还包括：

加密机在对预览节目的内容进行加密时，该预览节目的媒体报文生成附加段，并在所述附加段中根据该预览节目的预览规则设置该预览节目当前所处阶段的标识；且所述步骤C3具体包括：

终端中的DRM Agent根据所述的阶段标识和所述预览节目的CEK或生成CEK的种子解密各预览节目的媒体报文，实现IPTV节目的预览。

所述步骤C3具体包括：

终端中的DRM Agent 确认所述阶段标识为可预览阶段的标识后，根据获取的所述预览节目的CEK或生成CEK的种子解密各预览节目的媒体报文，实现IPTV节目的预览，或者，

当终端中的DRM Agent 确认所述预览节目的媒体报文附加段中所承载的阶段标识为不可预览阶段的标识后，终端根据所述节目的内容标识Content ID进行节目订购处理。

由上述本发明提供的技术方案可以看出，采用本发明所述的方法具有如下优点：

1、实现对批量节目进行预先授权，减少对版权中心的并发访问量，提高系统的可靠性；

2、由于实现了对批量节目进行预先授权，减少了用户从版权中心申请下发预览版权的次数，从而减少了用户等待时间，提高用户的体验；

3、可配置的预览规则为运营商提供了灵活的业务运营的方法，比如可以

将预览规则相同的多个节目进行打包发售；

4、本发明只需通过增加软件即可实现，能够很好地兼容现有设备。

附图说明

图1为本发明所述的方法的流程图。

具体实施方式

本发明的核心思想是：在OMA DRM加密系统中，建立预览组；并根据预览组为终端生成组授权信息，下发至终端；终端根据其接收的组授权信息，获取其从对应预览组中选择的各预览节目的CEK（Content Encrypt Key，内容加密密钥）或CEK的种子，并对其选择的各预览节目进行解密，实现IPTV节目的预览。

本发明技术方案的实现基于一个前提：预览节目的CEK或者生成CEK的种子是不变的，即在节目的整个播放过程中，CEK可以根据一个随机、但是固定的值依据某种算法获得。

为对本发明有进一步的了解，下面将结合附图对本发明所述的方法进行详细的说明。

本发明所述方法的具体实现方式如图1所示，包括以下步骤：

步骤11：在OMA DRM加密系统中，加密机根据不同的预览规则，为预览节目创建多个预览组，并且为每个预览组确定Group ID（组标识）、GEK（Group Encrypt Key，组加密密钥）等信息。

加密机创建预览组后，将预览组相对应的信息通知版权中心，版权中心保存关于预览组的相关信息。

其中预览规则是指对终端观看预览节目的约束，可以按照允许预览节目

的时间长度、次数或者有效期等约束进行划分。

这样，可以将每个预览节目根据各自的预览规则划分到相应的预览组中，一个预览组可以包括多个预览规则相同的预览节目。

步骤12：当某个节目允许预览时，对该节目进行加密处理。

本发明中需要对该节目进行两级加密处理，即对节目内容进行加密和对该节目的CEK或生成CEK的种子再进行加密处理。这两个加密过程可以连续进行，也可以分别单独进行。

对预览节目进行加密的过程是：

确定该预览节目的CEK或生成CEK的种子，采用对称加密算法对该节目的媒体报文进行加密处理。由于采用的是对称加密算法，所以该节目内容的解密密钥就是该节目的CEK或生成CEK的种子，解密算法就是相应的加密算法。

对预览节目的CEK或生成CEK的种子进行加密后的信息可以承载于节目的媒体描述信息（如果采用SDP协议，则是SDP文件）的ISMACrypKey（ISMA加密键）中。

下面详细介绍将预览节目的CEK或生成CEK的种子进行加密后的信息承载于节目的描述信息的ISMACrypKey中的加密过程，具体包括：

首先，加密机确定该预览节目的CEK；

然后，加密机根据该节目的预览规则从已经创建的预览组中选择相对应的预览组，获得该预览组的Group ID和GEK；

最后，在节目的媒体描述信息中的ISMACrypKey中定义参数GroupID和ContentKey（内容密钥），其中：

参数Group ID的值为：该节目相对应的预览组的Group ID；

参数Content Key的内容为：加密密钥为该节目相对应的预览组的GEK，采用对称加密算法对该节目的CEK或生成CEK的种子加密后获得的值，再进

行编码后的值;

由于采用的是对称加密算法, 因此, 该节目的CEK或生成CEK的种子的解密密钥就是相应预览组的组加密密钥GEK, 解密算法就是相应的加密算法。

ISMACrypKey的格式举例如下:

ISMACrypKey=(URL)http://10.164.22.58:6080/ri/servletcontentissuer?ContentID=019ba4422a285ebd;&GroupID=001;&ContentKey=:base64:YXVkcwAAEACAAACqADibcfgSerik7TpMjwF1hnXW5lcAAAAAAAAAAAAAAAAACBn

ISMACrypKey中的URL (Unique Resource Link, 唯一资源链接) 是指: 在用户确认订购节目后, 订购请求发送的地址。

另外, 加密机在对节目的内容进行加密时, 节目的媒体报文生成附加段, 并根据预览规则在附加段中设置该节目当前所处阶段的标识, 阶段标识包括:

可预览阶段的标识和于不可预览阶段的标识。

这样, 就可以根据该阶段标识来控制终端对预览节目内容的解密处理; 也就是说当阶段标识为可预览阶段的标识时, 允许终端对预览节目内容进行解密处理, 当阶段标识为不可预览阶段的标识时, 不允许终端对预览节目内容进行解密处理。

步骤13: 终端获取组授权信息, 并保存。

当终端完成到版权中心的注册后, 根据EPG (Electric Program Guide, 电子节目指南) 的通知, 根据本地保存的组授权信息情况向版权中心申请下发预览组的组授权信息;

版权中心根据终端的申请, 根据保存的相应预览组的信息以及终端的信息生成相应的组授权信息并下发给终端;

终端接收到版权中心下发的组授权信息后进行保存。

组授权信息包括：相应预览组的Group ID、该预览组所在的预览节目的CEK或生成CEK的种子的解密密钥（即组加密密钥GEK）及解密算法（即相应的加密算法）、预览规则以及申请组授权信息的终端信息等。

只有组授权信息中含有终端信息的目的是：只有符合该终端信息的终端才可以利用该组授权信息解密预览节目，防止组授权信息被盗而给运营商带来不利的影响。

终端获取组授权信息后，就获得了组授权信息相对应的预览组的所有节目的预览权利。因此，当终端以后选择属于该组授权信息对应的预览组的预览节目时，则不必再进行相应组授权信息的下发，这样，不但减少了对版权中心的并发访问量，提高了系统的可靠性；同时也减少了终端从版权中心申请下发预览版权的次数，从而减少了用户的等待时间；而且，运营商也可以将预览规则相同的多个节目进行打包发售。

步骤14：终端选择预览节目。

终端从EPG中获取节目列表，列表中有各个节目的URL、版权中心的URL和/或可预览标识等信息，当节目列表中含有可预览标识时，表明该节目可以预览。

终端根据节目列表选中某一节目，如果终端没有订购该节目，并且该节目是可预览的，则在界面提示预览或订购；

终端选择预览该节目。

步骤15：终端从MDN获取该预览节目的媒体描述信息。

步骤16：终端获取该预览节目的解密密钥。

终端根据获取的该节目的媒体描述信息中的ISMACrypKey中的参数Group ID的值，检索已经保存的组授权信息；

如果该预览节目相对应的组授权信息存在，则获得ISMACrypKey中的参数Content Key的解密密钥和解密算法信息，该解密密钥就是该预览节目相对

应的预览组的GEK，解密算法就是相应的加密算法，并根据该GEK和解密算法信息解密Content Key参数获得该预览节目的CEK或生成CEK的种子，即节目内容的解密密钥。

如果该预览节目相对应的组授权信息不存在，则终端根据该节目的描述信息中的ISMACrypKey中的参数Group ID向版权中心申请下发相应的组授权信息；

版权中心根据终端的申请生成相应的组授权信息并下发给终端；

终端将接收到的组授权信息进行保存，并获取参数Content Key的解密密钥GEK和解密算法信息，然后根据该GEK和解密算法信息解密Content Key参数获得该预览节目的CEK或生成CEK的种子，即节目内容的解密密钥。

步骤17：终端与媒体服务器建立连接，接收节目的媒体报文并解密。

如果终端接收到的媒体报文的附加段中的阶段标识为该节目当前处于可预览的阶段标识，则DRM Agent（代理）使用获得的该预览节目的CEK或生成CEK的种子对媒体报文进行解密，播放器播放节目，实现节目预览。

步骤18：终端订购预览节目。

如果终端接收到的媒体报文的附加段中的阶段标识为该节目当前处于不可预览的阶段标识，则DRM Agent根据相应节目的媒体描述信息中的ISMACrypKey中的Content ID（内容标识）检索终端中是否存在该节目的版权，如果不存在，则播放器暂停媒体报文的下发，并提示是否订购；

如果终端选择订购，则根据节目的描述信息中的ISMACrypKey中的URL，向版权中心发起订购请求；

当终端获得该节目的版权后，从版权中获得该节目的CEK和版权规则，建立解密环境；播放器继续下发媒体报文，DRM Agent继续接收加密的媒体报文，然后根据该节目的CEK或生成CEK的种子对媒体报文进行解密，节目正常播放。

如果终端选择不订购，则停止媒体报文的接收。

本发明的另外一种实施方案是：加密机将预览节目的CEK或生成CEK的种子的进行加密后的信息承载于节目的媒体报文（如果采用RTP协议，则是RTP报文）的附加段中，下发到终端；终端按照上述步骤16的方法从每个加密的媒体报文中获取节目内容的解密密钥，对媒体报文进行解密。

综上所述，采用本发明所述的方法，能够实现对批量节目进行预先授权，不但可以减少对版权中心的并发访问量，提高系统的可靠性；而且可以减少用户从版权中心申请下发预览版权的次数，从而减少了用户等待时间，提高用户的体验；另外，可配置的预览规则为运营商提供了灵活的业务运营的方法。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

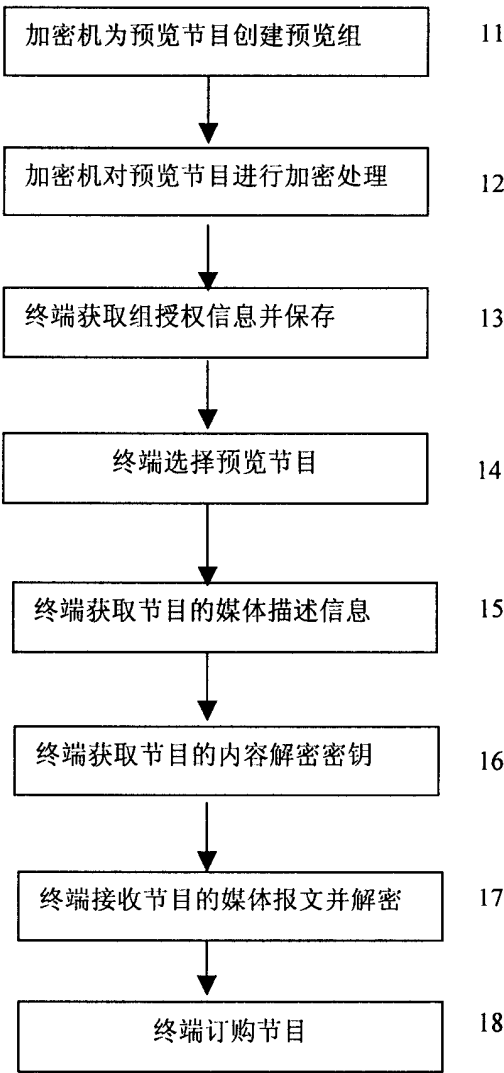


图1