(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101506790 B
(45)授权公告日 2013.04.03

(21)申请号 200680024443.8
(22)申请日 2006.06.22
(30)优先权数据
11/176,058 2005.07.07 US
(85)PCT申请进入国家阶段日
2008.01.07
(86)PCT申请的申请数据
PCT/US2006/024293 2006.06.22
(87)PCT申请的公布数据
WO2007/008362 EN 2007.01.18
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 A·帕卡 A·E·克莱门茨
E·P·奥利弗拉 S·巴哈塔
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈斌
(51)Int.Cl.
G06F 15/16(2006.01)

(56)对比文件
US 2004/0193680 A1,2004.09.30, 说明书第【0006】,【0024】,【0057】,【0064】-【0068】,【0110】-【0127】、摘要.
US 2003/0161473 A1,2003.08.28, 说明书【0053】,【0086】,【0148】,【0315】,【0341】-【0345】、附图9.
CN 1571999 A,2005.01.26, 全文.

审查员 赵晓春

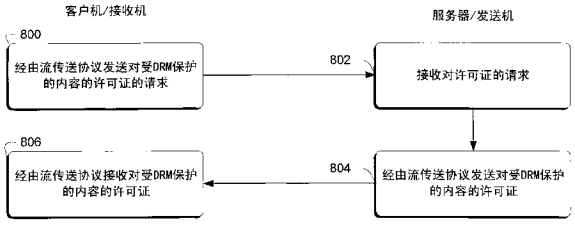
权利要求书 2 页 说明书 11 页 附图 9 页

(54)发明名称

承载使用用于流传送的控制协议和传输协议保护的内容

(57)摘要

各个实施例利用保护内容的各种方法,诸如数字权限管理(DRM),来允许在诸如家庭媒体网络等的局域网内的多个机器和设备上安全地回放内容。在至少某些实施例中,分别使用用于流传送的控制协议和传输协议来传递消息和内容。在至少某些实施例中,用于流传送的控制协议是实时流传送协议(RTSP),而传输协议为实时传输协议(RTP)。



CN 101506790 B

1. 一种用于承载受保护内容的计算机实现的方法，所述方法包括：

使用用于流传送的控制协议来建立用于交换受保护内容的控制流；

使用数据流来传输受保护内容，其中所述数据流使用一传输协议；

在所述受保护内容的流传送期间更新与所述受保护内容相关联的策略或格式信息，所述更新是经由 RTSP 通告请求来发送的，其中通告请求可承载包含新的 XMR 许可证的许可证响应消息，当策略和格式均改变时，将策略改变作为嵌入在 SDP 描述中的许可证响应请求发送。

2. 如权利要求 1 所述的方法，其特征在于，所述建立控制流的动作包括：

向被配置成发送所述受保护内容的发送机发送许可证请求消息；以及

从所述发送机接收包含一许可证的许可证响应消息。

3. 如权利要求 1 所述的方法，其特征在于，所述建立控制流的动作包括：

从被配置成播放所述受保护内容的接收机接收许可证请求消息；以及

向所述接收机发送包含一许可证的许可证响应消息。

4. 如权利要求 1 所述的方法，其特征在于，所述建立控制流的动作是使用 RTSP 实现的。

5. 如权利要求 4 所述的方法，其特征在于，所述建立控制流的动作还包括：

在 RTSP 描述请求的正文中向发送机发送许可证请求消息；以及

从所述发送机接收包括含有许可证的许可证响应消息的 RTSP 会话描述协议（SDP）。

6. 如权利要求 4 所述的方法，其特征在于，所述建立控制流的动作还包括：

从接收机接收 RTSP 描述请求的正文中的许可证请求消息；以及

向所述接收机发送包括含有许可证的许可证响应消息的 RTSP 会话描述协议（SDP）。

7. 如权利要求 1 所述的方法，其特征在于，所述传输的动作是使用 RTP 来实现的。

8. 如权利要求 1 所述的方法，其特征在于，所述更新的动作包括经由用于流传送的控制协议来接收更新。

9. 如权利要求 8 所述的方法，其特征在于，所述用于流传送的控制协议包括 RTSP，且所述更新是经由 RTSP 通告请求来接收的。

10. 一种用于承载受保护内容的计算机实现的方法，所述方法包括：

使用用于流传送的控制协议来建立用于交换受保护内容的控制流，所述控制协议是使用 RTSP 实现的；以及

使用数据流来传输受保护内容，其中所述数据流使用一传输协议，所述传输的动作是使用 RTP 来实现的；

在所述受保护内容的流传送期间更新与所述受保护内容相关联的策略或格式信息，所述更新是经由 RTSP 通告请求来发送的，其中通告请求可承载包含新的 XMR 许可证的许可证响应消息，当策略和格式均改变时，将策略改变作为嵌入在 SDP 描述中的许可证响应请求发送。

11. 如权利要求 10 所述的方法，其特征在于，所述传输的动作包括在包含经加密的受保护内容的 RTP 分组中包括可在将所述经加密的内容解密的解密过程中使用的加密参数。

12. 如权利要求 11 所述的方法，其特征在于，所述 RTP 分组可包含多个不同的经加密的有效负荷。

13. 如权利要求 12 所述的方法，其特征在于，所述加密参数包括用于每一经加密的有

效负荷的密钥 ID 扩展和初始化向量。

14. 如权利要求 10 所述的方法，其特征在于，所述传输的动作包括：

定义包含可在将经加密的受保护内容解密的解密过程中使用的加密参数的描述符；以及

使所述描述符与所述受保护内容相关联。

15. 如权利要求 14 所述的方法，其特征在于，所述关联的动作包括将所述描述符追加在所述 RTP 分组的尾部。

16. 如权利要求 14 所述的方法，其特征在于，所述经加密的受保护内容可使用由所述描述符引用的单个密钥来解密。

17. 如权利要求 10 所述的方法，其特征在于，所述传输的动作还包括：

在 RTSP 描述请求的正文中向发送机发送许可证请求消息；

从接收机接收所述 RTSP 描述请求的正文中的所述许可证请求消息；

向所述接收机发送包括含有许可证的许可证响应消息的 RTSP 会话描述协议（SDP）；

从所述发送机接收包括含有所述许可证的所述许可证响应消息的所述 RTSP 会话描述协议（SDP）。

承载使用用于流传送的控制协议和传输协议保护的内容

[0001] 背景

[0002] 数字权限管理 (DRM) 指的是用于诸如通过控制或限制对数字媒体内容在电子设备上的使用来保护内容的技术。DRM 的一个特性在于，它可将媒体内容绑定到给定的机器或设备。因此，一般将关于特定内容并定义与该内容相关联的权限和限制的许可证绑定至该给定的机器或设备。因此，用户一般不能够取得该内容，并将其移动至另一机器以便回放该内容。

[0003] 存在许可受到 DRM 保护的内容被移动至其它机器以便于在这些机器上回放该内容的某些技术，但这些技术倾向于使用不适于同时传送和回放内容的非实时内容传送协议。

[0004] 概述

[0005] 各种实施例利用保护内容的各种方法，诸如数字权限管理 (DRM)，来允许在诸如家庭媒体网络等的局域网内的多个机器和设备上安全地回放内容。在至少某些实施例中，分别使用用于流传送的控制协议和传输协议来传递消息和内容。在至少某些实施例中，用于流传送的控制协议是实时流传送协议 (RTSP)，而传输协议为实时传输协议 (RTP)。

[0006] 附图简述

[0007] 图 1 示出了可用其来在一个实施例中采用本发明实施例的一协议的示例性注册过程。

[0008] 图 2 示出了可用其来在一个实施例中采用本发明实施例的一协议的示例性邻近检测过程。

[0009] 图 3 示出了可用其来在一个实施例中采用本发明实施例的一协议的示例性会话建立过程。

[0010] 图 4 示出了可用其来在一个实施例中采用本发明实施例的一协议的示例性数据传送过程。

[0011] 图 5 示出了可用其来根据一个实施例来利用本发明实施例的流传送协议的各个方面。

[0012] 图 6 示出了结合一个实施例来利用的图 5 中的流传送协议。

[0013] 图 7 示出了结合一个实施例来利用的图 5 中的流传送协议。

[0014] 图 8 是描述根据一个实施例的一方法中各步骤的流程图。

[0015] 图 9 示出了根据一个实施例的分组。

[0016] 图 10 示出了根据一个实施例的样本加密。

[0017] 图 11 示出了根据一个实施例的分组。

[0018] 详细描述

[0019] 概观

[0020] 此处描述的各个实施例利用了用于保护内容的各方法，诸如数字权限管理 (DRM) 以允许在诸如家庭媒体网络的局域网内的多个机器和设备上安全地回放内容。在至少某些实施例中，分别使用用于流传送的控制协议和传输协议来传递消息和内容。在至少某些

实施例中，用于流传送的控制协议为实时流传送协议 (RTSP)，而传输协议为实时传输协议 (RTP)。如由本领域的技术人员所理解的，在这些实施例中，引入了协议扩展，它们享受由 RTSP/RTP 提供的优点，包括通过用户数据报协议 (UDP) 和客户机与服务器之间的双向通信来进行数据传递。

[0021] 具体地，在至少某些实施例中，协议扩展使用 RTSP 安全地建立一会话，传输用 RTP 封装的受保护数据，提供根据 RTP 有效负荷格式来加密和传送数据的各种方案，以及用于同经加密的内容数据一起传送加密参数的各种方法。

[0022] 在以下的讨论中，提供了题为“内容安全和许可证传送协议的章节，它描述了可在其中采用本发明技术的一个特定系统。在其之后，提供了题为“RTSP”的章节以向不熟悉 RTSP 的读者给出 RTSP 领域中用于理解本发明技术的至少某些上下文。在该章节之后，提供了题为“使用 RTSP 的示例性实现”的章节，它描述了采用 RTSP 以建立控制流并利用 RTP 来建立数据流的各种本发明技术。

[0023] 内容安全和许可证传送协议

[0024] 以下提供了一示例性协议的讨论，该协议提供用于内容通过数字链路流动的安全和传送许可证。该协议仅构成了可用其来采用各种发明的技术的一个示例性协议。可以理解和领会，可利用其它协议，而不背离所要求保护的本主体的精神和范围。

[0025] 在描述中使用以下密码记号：

[0026] K{数据} 使用秘密密钥 K 来加密数据。

[0027] K[数据] 使用秘密密钥 K 来签署数据。

[0028] $\{数据\}_{设备}$ 用设备的公钥来加密数据。

[0029] $[数据]_{设备}$ 用设备的私钥来签署数据。

[0030] 在此特定协议中，有五个主要过程：注册、重新验证、邻近检测、会话建立、和数据传送。

[0031] 在注册过程中，发送机（即，有内容要发送给另一设备的一设备）可唯一且安全地表示预期的接收机（即，要向其发送内容的设备）。在该特定协议中，发送机维护具有已注册接收机的数据库，并确保不同时使用超过少量预定数目的接收机。在该注册过程期间，发送机还采用邻近检测过程来确保接收机位于网络中发送机的“附近”，以防止受保护内容的广泛分发。

[0032] 重新验证过程被用来确保接收机继续在发送机“附近”。除非接收机在过去的一预定时间段内已注册或已重新验证，否则内容不被传递给该接收机。

[0033] 只要接收机向发送机请求内容就使用会话建立过程。发送机强制在完成会话建立之前该设备必须经过注册或最近经过验证。

[0034] 一旦建立了会话，所请求内容的数据传送可用安全的方式进行。接收机可再次使用该会话来检索该内容的特定部分（查找），但必须建立一新会话以便检索不同的内容。

[0035] 现在结合图 1 和描述注册期间在发送机和接收机之间传递的各个消息的下表来考虑注册过程。

[0036]

消息	值	描述
注册请求消息	Ver（版本）	8 位协议版本
	Cert（证书）	接收机的 XML 数字证书。
	DId（设备 Id（标识））	128 位序列号。
注册响应消息	Ver（版本）	8 位协议版本
	{种子}设备	用于导出内容加密密钥和内容完整性密钥的 128 位种子。
	SN（序列号）	128 位序列号
	地址	发送机传入和传出的邻近分组套接字的地址。
	SId（会话 Id）	128 位随机会话 Id。
邻近检测算法		在频带外执行邻近检测算法。

[0037] 此处，接收机发送除其它信息外还包含接收机的数字证书的注册请求消息。响应于接收该注册请求消息，发送机验证接收机的证书，生成种子和随机会话 ID，在注册响应消息中按上述格式向接收机返回同样内容。接收机然后验证发送机的签名，获取会话 ID 并执行附图中所示的其它动作。接收机和发送机然后可经历以下描述的邻近检测过程。

[0038] 对于重新验证，执行与上述相同的过程，区别在于，在重新验证期间，接收机已在数据库中注册。

[0039] 对于邻近检测，结合图 2 考虑以下。

[0040] 在邻近检测过程期间，接收机向发送机发送包含邻近检测初始化消息中指示的会话 Id 的消息。发送机然后向接收机发送包含现时值 (Nonce)(128 位随机值) 的消息，并测量接收机以使用内容加密密钥加密的现时值来答复所花的时间。最后，发送机向接收机发送指示邻近检测成功与否的消息。

[0041] 接收机可重复该过程，直到它确认邻近检测成功。当该特定协议在基于 IP 的网络上使用时，通过 UDP 来交换邻近检测消息。接收机经由注册响应消息知道发送机的地址。接收机的地址不需要单独传送，因为可通过检查承载邻近检测初始化消息的 UDP 分组的传入 IP 头来确定。

[0042] 下表描述了在邻近检测期间交换的消息 ：

[0043]

消息	值	描述
邻近开始消息	SId（会话 Id）	由发送机发送的同一 128 位会话 Id 值。
邻近质询消息	Seq（序号）	8 位递增序号。
	SId（会话 Id）	同一 128 位会话 Id。
	现时值	128 位随机值。
邻近响应消息	Seq（序号）	由发送机确定的同一序号。
	SId（会话 Id）	同一 128 位会话 Id。
	KC{现时值}	使用内容加密密钥加密的 128 位现时值。
邻近结果消息	SId（会话 Id）	同一 128 位会话 Id。
	结果	指示注册过程成功还是失败的状态码。

[0044] 对于会话建立，结合图 3 和描述在会话建立期间交换的消息的下表考虑以下。

[0045]

消息	值	描述	
许可证请求消息	Ver（版本）	8 位协议版本	
	Cert	接收机的 XML 数字证书。	
	SN（序列号）	128 位序列号。	
	动作	请求的内容使用。例如：“播放”、“复制”或“烧录”。	
	RId（权限 Id）	128 位随机权限 Id。	
	VCRL（CRL 版本）	接收机 CRL 的版本。	
许可证响应消息	Ver（版本）	8 位协议版本	
	CRL	发送机的 CRL。仅在发送机具有高于接收机的 CRL 的版本号且接收机组件也具有发送能力时才发送。	
	许可证	KC (用接收机的公钥加密)	128 位随机内容加密密钥。
		KI (用接收机的公钥加密)	128 位随机内容完整性密钥。
		VCRL（CRL 版本）	发送机的 CRL 版本
		RId（权限 Id）	由接收机发送的同一 128 位随机权限 Id。
		SN（序列号）	128 位序列号。

[0046] 在此示例中，从接收机向发送机发送许可证请求消息，它包含上述信息。作为响应，发送机可发送包含上述信息的许可证响应消息。

[0047] 在该特定示例中，用 XMR 格式表示许可证，许可证包括内容加密密钥、内容完整性密钥、发送机 CRL 的版本、128 位权限 Id 和 128 位序列号。许可证还包含使用 OMAC 用内容完整性密钥计算的 OMAC。

[0048] 对于数据传送过程，结合图 4 考虑以下。一旦会话建立完成，即以控制协议专用的方式执行数据传送。数据传送请求和响应两者必须为控制协议和内容类型特别定义。这概念性地表示在图 4 中。

[0049] 现在提供了可用其来采用本发明实施例的示例性协议的简要概观，现在考虑 RTSP 的一些背景信息。

[0050] RTSP

[0051] 如本领域的技术人员所理解，实时流传送协议即 RTSP 是用于对具有实时特性的数据传递（即流传送）进行控制的应用层协议。RTSP 提供允许对诸如音频和视频的实时数据进行受控、按需传递的可扩展框架。数据源可包括实况数据馈送和已存储的剪辑两者。该协议旨在控制多个数据传递会话，提供用于选择诸如 UDP、组播 UDP 和 TCP 的传递信道的手段，并提供用于基于 RTP 选择传递机制的手段。

[0052] RTSP 建立并控制单个或多个时间同步的连续媒体流，诸如音频和视频。它自己一般不传递连续流，尽管连续媒体流与控制流的交织是可能的。换言之，RTSP 用作多媒体服务器的“网络遥控器”。

[0053] 要被控制的流的集合由演示描述定义。在 RTSP 中，不存在 RTSP 连接的概念；相反，服务器维护由标识符标记的会话。RTSP 会话决不绑定至传输层连接，诸如 TCP 连接。在 RTSP 会话期间，RTSP 客户机可打开或关闭至服务器的众多可靠的传输连接以发出 RTSP 请求。或者，如本领域的技术人员可以理解，可使用诸如 UDP 的无连接传输协议。

[0054] 由 RTSP 控制的流可使用 RTP，但 RTSP 的操作不依赖于用于承载连续媒体的传输机制。

[0055] 现在结合图 5 考虑客户机 / 接收机 500 与服务器 / 发送机 502 之间的典型的 RTSP 请求 / 响应交换。

[0056] 初步地，RTSP 请求 / 响应具有为简洁起见未做描述的标头。在 RTSP 中，客户机 / 接收机 500 一般发出被称为描述的请求，它针对从服务器 502 检索由请求 URL 标识的演示或媒体对象的描述。服务器 502 用以会话描述协议 (SDP) 表示的被请求资源的描述作出响应。描述响应 (SDP) 包含其所描述的资源的所有媒体初始化信息。

[0057] 接着，客户机 500 发送对指定要用于流传送媒体的传输机制的 URI 的设置请求。在图 5 的示例中，为音频和视频两者发送设置请求。客户机 500 还在设置请求中指示它将利用的传输参数。设置请求中的传输标头指定客户机可接受用于数据传输的传输参数。来自服务器 502 的响应包含由服务器所选的传输参数。服务器还响应于该设置请求生成会话标识符。

[0058] 此时，客户机可发出播放请求，它告知服务器以经由设置中指定的机制来开始发送数据。响应于接收播放请求，服务器可开始流传送内容，在此示例中，该内容为音频 / 视频内容。如本领域的技术人员可以理解，在此示例中，流传送的内容使用 RTP 分组封装并通

过 UDP 发送。

[0059] RTSP 协议具有感兴趣的其它方法，包括暂停、拆卸、获取参数、设置参数、重定向和记录。对关于 RTSP 的其它背景，读者应查询 1998 年 4 月的 RTSP 草案，Schulzrinne，H.，Rao，A. 和 R. Lanphier 的“Real Time Streaming Protocol（实时流传送协议）(RTSP)”，草案 2326，可在 http://www.ietf.org/rfc/rfc2326.txt 提供。

[0060] 使用 RTSP 的示例性实现

[0061] 在以下讨论中，有两个主要的子章节，一个题为“控制流”，描述如何使用 RTSP 建立受 DRM 保护的内容的控制流，另一个题为“数据流”，描述了如何使用 RTSP 建立受 DRM 保护的内容的数据流。这些主要子章节中的每一个都具有与之相关联的描述本发明的实施例的各方面的子章节。

[0062] 在以下讨论中，提供了如何根据一个实施例使用 RTSP/RTP 来实现上述协议的会话建立和数据传送过程的描述。更具体地，在以下的“控制流”章节中，提供了如何使用 RTSP 实现会话建立的描述。在“数据流”章节中，提供了如何使用 RTP 实现数据传送的描述。

[0063] 控制流

[0064] 根据该实施例，由希望回放受 DRM 保护的内容——即，具有相关联许可证的内容的接收机设备发起会话建立。回想以上对内容安全和许可证协议的讨论，客户机 / 接收机可相应地向服务器 / 发送机发送许可证请求消息，服务器 / 发送机可以许可证响应消息来对其答复。许可证响应消息又承载一许可证，在以上示例中该许可证是以可扩展媒体权限 (XMR) 来表示的。许可证包含与所请求的内容相关联的策略和内容密钥。

[0065] 在描述请求中承载许可证请求消息

[0066] 现在结合图 6 考虑内容安全和许可证协议与 RTSP 的汇合。具体地，图 6 示出了根据一个实施例的客户机 / 接收机 600 和服务器 / 发送机 602。根据该实施例，当客户机 / 接收机 600 希望访问受 DRM 保护的内容时，客户机在描述请求的正文中插入许可证请求消息。

[0067] 仅作为一个实现示例，考虑以下根据一个实施例包括许可证请求消息的描述请求消息摘录。

[0068] DESCRIBE rtsp://eduardo01/file.wmv RTSP/1.0

[0069] Accept :application/sdp

[0070] CSeq :1

[0071] Supported :com.microsoft.wmdrm-nd，com.microsoft.wm.eosmsg，

[0072] method.announce

[0073] Require :com.microsoft.wmdrm-nd

[0074] Content-Type :application/vnd.ms-wmdrm-license-request

[0075] Content-Length :1078

[0076] License_Request_Message

[0077] 在该示例中使用“Require（要求）:com.microsoft.wmdrm-nd”以指示接收机期望服务器为特定类型的发送机。在该示例中使用“Content-Type（内容类型）:application/vnd.ms-wmdrm-license-request”以指示该描述的正文包含许可证请求消息。

[0078] 除非存在错误，否则发送机应以 SDP 描述来答复，该描述包括在下一章节中描述的许可证响应消息。

[0079] 将许可证响应消息嵌入到 SDP 描述中

[0080] 接收到在正文中包含许可证请求消息的描述请求之后，服务器可返回许可证响应消息。在此示例中，服务器返回不仅包含前述各个参数而且包含许可证响应消息的 SDP 描述。在此实施例中，如前所述，许可证响应消息将承载指定将对内容应用哪些策略的 XMR 许可证。

[0081] 仅作为一个实现示例，考虑以下根据一个实施例包括许可证响应请求的 SDP 摘录。

[0082] RTSP/1.0 200 OK

[0083] Last-Modified :Thu,19 Dec 2002 15:36:18 GMT

[0084] Content-Length :1891

[0085] Content-Type :application/sdp

[0086] CSeq :1

[0087] Supported :com.microsoft.wmdrm-nd,com.microsoft.wm.eosmsg,

[0088] method.announce

[0089] SDP_Description

[0090] 根据一个实施例，由发送机返回的 SDP 包括根据 2397 草案 (http://www.ietf.org/rfc/rfc2397.txt) 的规范被编码在数据 URL 中的许可证响应消息。在一个示例中，包含在数据 URL 中的数据必须是 Base64 编码的，且 MIME 类型必须被设置为“application/vnd.ms-wmdrm-license-response”。

[0091] 作为句法的示例，考虑以下 :data :application/vnd.ms-wmdrm-license-response ;base64, AggAAAAAAAABOFhNUgAAAAAB+TTbzXCRwls+/jA4fQQY0wADAAEAAAEgAAMAAgAAADwAAQADAAAAEgBkAAAAAAAAAAAAAQAMAAAAGKRuHVtxsJ1Lk7WPrQPe5X0AAQANAAAACgABAAMABAAAABoAAQAFAAAAEgBkAGQAZABkAGQAAwAJAAAApgABAAoAACeajiAiUBMGrAGUAOIqMGBggABAAEAgC7V1QF54EzuYbTYKPbgBEK6nDXGtbV+bJKF+Cn2yd/FUaC4vTIOxkF/eQLx+FqvLCUMtxvRSw01dns9Ejt021se2T+IROiZA0t5pRuNl3gq7JK9JKs+ZX8hKsEJFW0V7cyp9wdaCMh2esJ97r9agH1Sxf0mAqcQ0j1Q5dtX1Wx/AAEACwAAABwAAQAQZZaX5nGEUAV8w6p6BQr++Q ==

[0092] 在该示例中，根据 SDP 密钥管理扩展规范，数据 URL 必须使用“a = key-mgmt”属性被插入到 SDP 会话层，该规范迄今为止仍是进展中的工作。句法如下 :a = key-mgmt : wmdrm-nd URL

[0093] URL 参数为上述数据 URL。

[0094] 在通告 (announce) 请求中承载许可证响应消息

[0095] 现在考虑一些媒体文件包含需要实施不同策略的片段。作为示例，采取由 Windows 媒体中心 TV 录制版生成的文件的情况。这样的文件受到 WMDRM 的保护，并具有与之相关联的多个策略。例如，对 TV 演出可能要求 Macrovision，但对出现在同一录制内的商业广告片段则不需要。

[0096] 该要求导致需要定义用于在流中间传递经更新的策略的机制。根据一个实施例，可使用 RTSP 的通告请求在流中间传递经更新的策略。在此实施例中，通告请求可承载包含新的 XMR 许可证的许可证响应消息。

[0097] 在此示例中，有两种与流传送媒体相关联的策略可能改变的情况。在第一种情况中，仅与特定流相关的策略可能改变。第二种情况中，策略和内容格式本身均可改变。

[0098] 考虑其中仅与流传送媒体相关联的策略可能改变的第一种情况。该情况的一个示例为 TV 演出片段与商业广告之间的切换，其中 TV 片段需要在模拟输出上启用 Macrovision，而商业广告不需要。注意到，在该示例中，仅策略改变：诸如比特率、编解码器等编码参数保持不变。

[0099] 考虑其中策略和内容格式两者均改变的第二种情况。该情况的一个示例也是 TV 演出片段与商业广告之间的切换，对策略有相同类型的改变。然而，在该示例中，TV 演出和商业广告是使用不同编码参数编码的，诸如从高清晰度编码过渡到标准清晰度编码。这样的场景一般被命名为“格式改变”。该情况的另一示例涉及通常被称为“条目改变”的情况。条目改变一般是在作为“服务器方播放列表”的一部分由服务器传递的媒体文件之间切换的结果。这些播放列表一般由不必共有任何编码参数或策略的媒体文件的集合组成。

[0100] 只要策略改变时格式未变，如在第一种情况中示出，服务器仅将新策略发送给客户机，作为通告请求的正文的一部分。在这种情况中，许可证响应消息被包括在通告消息的正文中。作为示例，考虑图 7，它示出了示例性的客户机 / 接收机 700 和向客户机 / 接收机发出通告请求以续接 (articulate) 带有经更新策略的新许可证的服务器 / 发送机 702。

[0101] 只要策略改变且格式改变，如第二种情况中所示，服务器向客户机传递经更新的 SDP 描述。要求该 SDP 描述以描述发生的格式改变。在该示例中，SDP 描述在格式改变的情况中也被作为通告请求传递。因此代替传递其中一个包含格式改变、另一包含策略改变的两个连续通告请求，服务器可仅发送承载 SDP 描述的一个通告请求。然后将策略改变作为嵌入在 SDP 描述中的许可证响应请求发送。再次考虑图 7，它示出了其正文包含具有嵌入的许可证响应消息的经更新 SDP 的通告请求。

[0102] 用于将许可证响应消息嵌入到作为通告请求的一部分的 SDP 描述中的格式与前述用于嵌入作为描述响应的一部分的 SDP 描述的格式相同。

[0103] 图 8 是描述根据一个实施例的方法中各步骤的流程图。该方法可结合任何合适的硬件、软件、固件或其组合来实现。在一个实施例中，该方法被实现为具体化成某种类型的计算机可读介质的一组计算机可读指令或软件代码。

[0104] 步骤 800 试图通过经由流传送协议发送对受 DRM 内容的许可证的请求来建立控制流。在所示和所述实施例中，该步骤由客户机 / 接收机执行。对许可证的请求的一个具体示例为上述的许可证请求消息。可利用其它的请求类型或格式，而不背离所要求保护的主题的精神和范围。此外，以上描述了流传送协议的一个示例 (即，RTSP)。可使用其它流传送协议，而不背离所要求保护的主题的精神和范围。在 RTSP 实施例中，将请求插入描述请求的正文内。

[0105] 步骤 802 试图通过接收该对许可证的请求来建立控制流。该步骤在此示例中由服务器 / 发送机实现。响应于接收请求，步骤 804 可使用流传送协议向客户机 / 接收机发送许可证。以上提供了将许可证返回给客户机 / 接收机的一个具体示例，其中向客户机 / 接收机发送了许可证响应消息形式的许可证。可利用其它响应类型或格式，而不背离所要求保护的主题的精神和范围。此外，以上描述了流传送协议的一个示例 (即，RTSP)。可利用其他流传送协议，而不背离所要求保护的主题的精神和范围。在 RTSP 实施例中，响应是用

SDP 发送的。

[0106] 可以理解和领会，步骤 804 也可被实现成向客户机 / 接收机发送更新。在此情况和 RTSP 示例的上下文中，可使用上述通告请求来传递更新。

[0107] 步骤 806 经由流传送协议接收许可证。在所示和所述实施例中，该步骤由客户机 / 接收机实现。在接收许可证之后，客户机可根据许可证中定义的条款来访问并消费内容。

[0108] 以下描述跟随许可证获取过程的数据流。

[0109] 数据流

[0110] 描述了结合受 DRM 保护的内容利用 RTSP 的控制流的示例性实施例，现在考虑包含实际受 DRM 保护的内容或允许其通信的数据流。

[0111] 在以下描述的实施例中，使用 RTP 作为数据传送协议在发送机和接收机之间传输受 DRM 保护的内容。即，受 DRM 保护的内容传输自发送机并传输至接收机。

[0112] 在提供的特定示例中，描述了两种不同的方法。在第一种方法中，所利用的 RTP 有效负荷格式支持扩展，进而允许诸如密钥 ID 扩展和初始化向量的加密参数被包括在 RTP 分组中，使得经加密的有效负荷数据可经历解密过程并被解密。在第二种方法中，RTP 有效负荷格式不支持扩展。因此，在该方法中，定义了描述符，它与包含经加密的有效负荷的 RTP 分组相关联。描述符包含诸如密钥 ID 扩展和初始化向量等可在解密过程中使用来对经加密的有效负荷数据解密的加密参数。

[0113] 通过 Windows 媒体有效负荷格式来承载样本加密的有效负荷

[0114] 图 9 示出了根据一个实施例、整体在 900 处的 RTP 分组的示例性部分。在该实施例中，所利用的 RTP 有效负荷格式以允许诸如密钥 ID 扩展和初始化向量等的加密参数连同经加密的有效负荷内容一起被包括在 RTP 分组中的方式来支持扩展。这样的格式的一个示例为 Windows 媒体 RTP 有效负荷格式，它在 http://download.microsoft.com/download/5/5/a/55a7b886-b742-4613-8ea8-d8b8b5c27bbc/RTPPayloadFormat_for_WMAandWMV_v1.doc 描述。然而，可利用其他格式，而不背离所要求保护的主题的精神和范围。

[0115] 在该示例中，分组 900 包括 RTP 标头 902 和有效负荷格式标头 904。有效负荷格式标头在该示例中允许扩展。因此，分组 900 还包括密钥 ID 扩展 906 和初始化向量 908，以及与密钥 ID 扩展 906 和初始化向量 908 相关联并可用其来解密的经加密有效负荷数据 910（音频或视频数据中任一）。此外，RTP 分组 900 可包括多个其它经加密的有效负荷。在此特定示例中，分组 900 还包括另一有效负荷格式标头 904a、密钥 ID 扩展 906a、初始化向量 908a、以及与密钥 ID 扩展 906a 和初始化向量 908a 相关联并可用其来解密的经加密有效负荷数据 910a（音频或视频数据中任一）。

[0116] 在该特定实施例中，一个 RTP 分组可包含多个不同的经加密的有效负荷。作为仅在一个特定上下文中的特定实现示例，结合 Windows 媒体音频和视频内容考虑以下。

[0117] 当承载受上述许可证保护的 Windows 媒体内容时，必须在 RTP 分组中设置以下值和字段。

[0118] 1. “MAU 属性”部分中位字段 (Bit Field)2 中的“加密”位 (E) 必须被设置为 1。

[0119] 2. “MAU 定时”部分中“扩展存在”位 (X) 必须为设置为 1，以指示扩展字段的存在性。

[0120] 3. “经加密有效负荷边界”扩展不允许存在。

[0121] 4. 必须包括“WMDRM 初始化向量”扩展。以下值必须被设置：

[0122] a. “扩展类型”必须被设置为 2。

[0123] b. “扩展长度”必须被设置为 8(意为 64 位)。

[0124] c. 必须用如以下在题为“样本加密”的章节中定义的样本 ID 值来设置“扩展数据”。

[0125] d. 必须为每个 MAU 的第一有效负荷包括该扩展。如果 MAU 被分成多个有效负荷，则该扩展应仅存在于第一有效负荷中。

[0126] 5. 必须包括“WMDRM 密钥 ID”。以下值必须被设置：

[0127] a. “扩展类型”必须被设置为 3。

[0128] b. “扩展长度”必须被设置为 16(意为 128 位)。

[0129] c. 在承载 ASF 内容时必须用来自 ASF 内容加密对象的密钥 ID 值来设置“扩展数据”。或者，在承载诸如 DVR-MS 的非 ASF 内容时，它被设置为表示所使用的加密密钥的密钥 ID 值。

[0130] d. 必须为每个多有效负荷 RTP 分组中的第一有效负荷包括该扩展以解决分组丢失问题。

[0131] 样本加密

[0132] 作为对以上项目 4(c) 的进一步解释，考虑以下。在该实施例中，每一样本应使用计数器模式的 AES 加密。图 10 示出了用于使用该技术对单个样本加密的过程。

[0133] 在该实施例中，计数器模式创建字节流，这些字节然后与媒体样本的明文字节异或 (XOR) 以创建经加密的媒体样本。密钥流生成器使用 AES 轮来一次生成 16 字节块的密钥流。对 AES 轮的输入为内容加密密钥 (K_C) 以及样本 ID 与样本内块号的 128 位级联。

[0134] 密钥流生成器的输出应与来自媒体样本的相应块 (i) 的数据逐个字节地异或。在媒体样本未被按 16 字节平均划分的情况中，仅来自最后一块的媒体数据的有效字节应与密钥流异或并被保留为经加密的样本。

[0135] 当加密来自 ASF 文件的样本时，样本 ID 等效于来自有效负荷扩展的样本 ID。

[0136] 因此，在该实施例中，根据“样本”边界来加密和解密数据，这些边界是给定媒体类型的自然边界，例如视频流的视频帧或音频流的音频样本块。

[0137] 使用数据片段描述符通过 RTP 有效负荷格式来承载链路加密的有效负荷

[0138] 图 11 示出了根据另一个实施例、整体在 1100 处的分组的各个方面。在该示例中，分组 1100 可包括 IP 标头 1102、UDP 标头 1104、RTP 标头 1106、有效负荷格式标头 1108、有效负荷数据 1110 和描述符 1112。在该特定示例中，将描述符追加到有效负荷数据的尾部，尽管它可被置于任何合适的位置。如本领域的技术人员可以理解的，将描述符置于有效负荷数据的尾部可减轻后向兼容问题。

[0139] 在该实施例中，除 RTP 标头以外的 RTP 分组被视为与描述符 1112 相关联的数据片段来处理。描述符 1112 又承载了可在能够解密有效负荷数据 1110 的解密过程中使用的加密参数。在该特定实施例中，对有效负荷数据 1110 应用了单个策略和内容加密密钥。

[0140] 根据一个实施例，描述符 1112 包括如下的数据结构：

[0141]

部分	字段
标志	8 位标志
扩展	8 位扩展个数
	多个可变长度扩展
长度	数据片段描述符长度

[0142] 在该示例中，标志部分为指示数据属性的位字段。当前定义以下值：0x01 指示经加密数据。当该标志被置位时，它指示数据处于加密形式。否则，该数据为明文。

[0143] 对于扩展部分，扩展个数字段指示包括在该描述符中的可变长度扩展的个数。对于可变长度扩展字段，每一扩展具有以下格式：

[0144]

字段
8 位扩展类型
16 位扩展长度
可变长度扩展

[0145] 根据一个实施例，密钥 ID 扩展和数据片段 ID 扩展被如下定义：

[0146] 密钥 ID 扩展

[0147] 扩展类型：对于密钥 ID 扩展，必须被设置为 0x01。

[0148] 扩展长度：必须被设置为 16，表示 128 位（16 字节）。

[0149] 扩展：必须包含同该描述符一起传递的经加密媒体的密钥 ID 值。该扩展仅在加密数据标志被置位时才使用。

[0150] 数据片段 ID 扩展

[0151] 扩展类型：对于数据片段 ID 扩展，必须被设置为 0x02。

[0152] 扩展长度：必须被设置为 8，表示 64 位（8 字节）。

[0153] 扩展：必须包含同该描述符一起传递的经加密媒体的数据片段 ID 值。该扩展仅在加密数据标志被置位时才使用。

[0154] 对于长度部分，在该实施例中，该部分必须包含以字节为单位的数据片段描述符的总长度。该长度并不包括同该描述符一起传递的媒体数据的大小。

[0155] 结论

[0156] 上述各个实施例利用保护内容的各种方法，诸如数字权限管理（DRM）来允许在诸如家庭媒体网络的局域网内的多个机器和设备上安全地回放内容。在至少某些实施例中，经由实时流传送协议（RTSP）和实时传输协议（RTP）来传递消息和内容，且引入了协议扩展，它享受由 RTSP/RTP 提供的优点，包括通过用户数据报协议（UDP）以及客户机与服务器之间双向通信来进行数据传递。

[0157] 尽管用结构特征和 / 或方法步骤专用的语言描述了本发明，但可以理解，所附权利要求书中定义的本发明不必限于所述的特定特征或步骤。相反，特定特征和步骤被公开为实现所要求保护的本发明的优选形式。

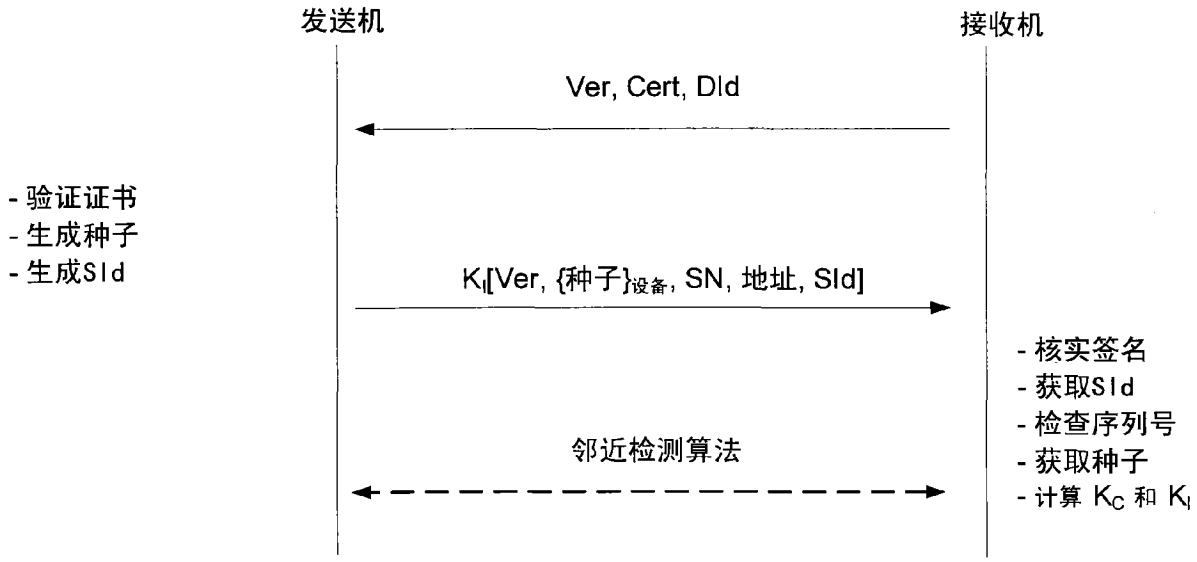

发送机
接收机
Ver, Cert, DId
- 验证证书
- 生成种子
- 生成SId
K_I[Ver, {种子}设备, SN, 地址, SId]
- 核实签名
- 获取SId
- 检查序列号
- 获取种子
- 计算 K_C 和 K_I
邻近检测算法

图 1

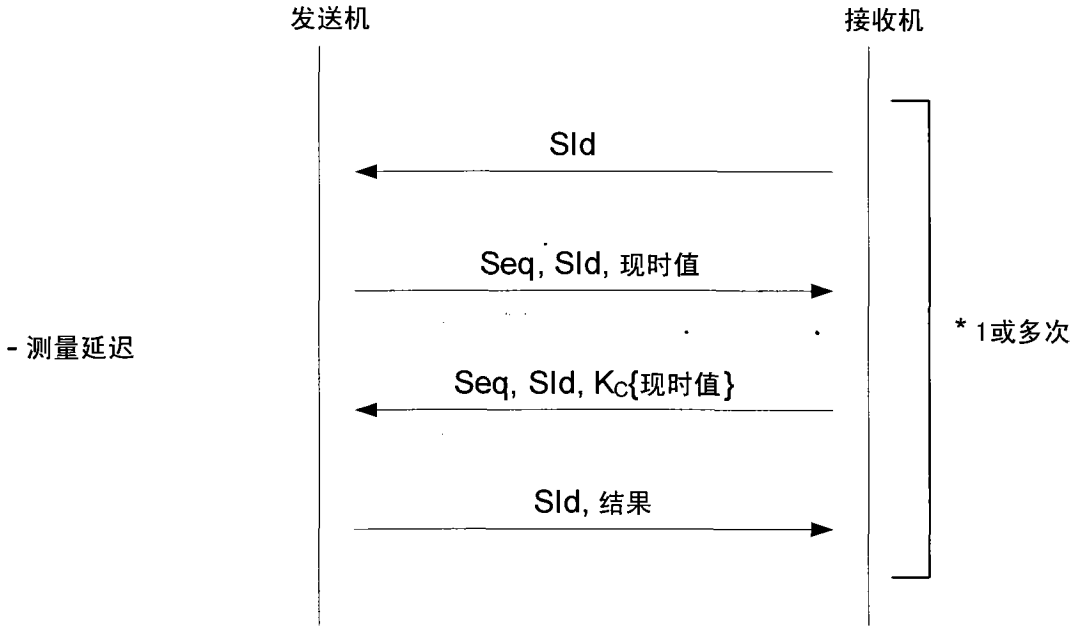

发送机
接收机
SId
Seq, SId, 现时值
- 测量延迟
* 1或多次
Seq, SId, K_C{现时值}
SId, 结果

图 2

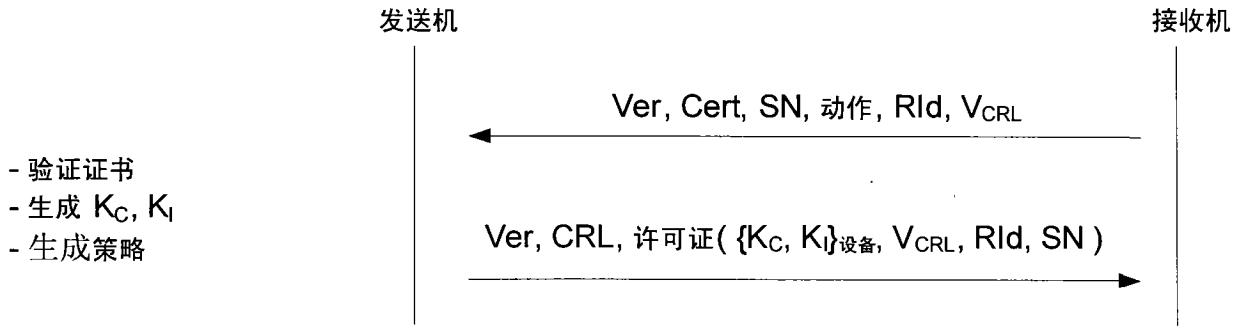

发送机
接收机
Ver, Cert, SN, 动作, RId, V_{CRL}
- 验证证书
- 生成 K_C, K_I
- 生成策略
Ver, CRL, 许可证($\{K_C, K_I\}_{设备}$, V_{CRL}, RId, SN)

图 3

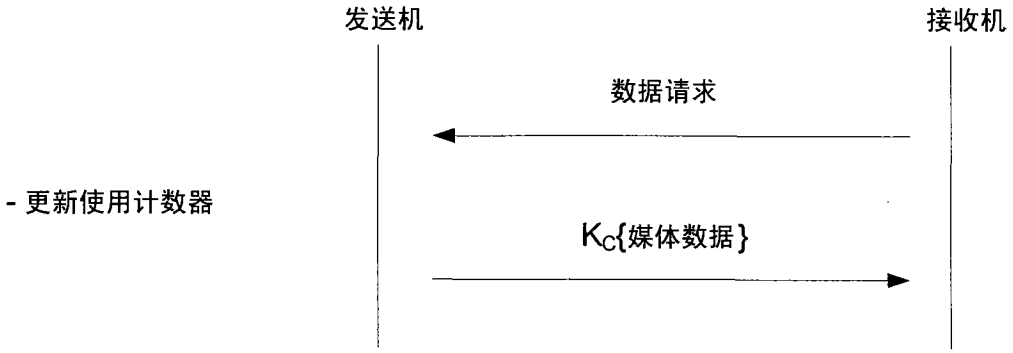

发送机
接收机
数据请求
- 更新使用计数器
K_C{媒体数据}

图 4

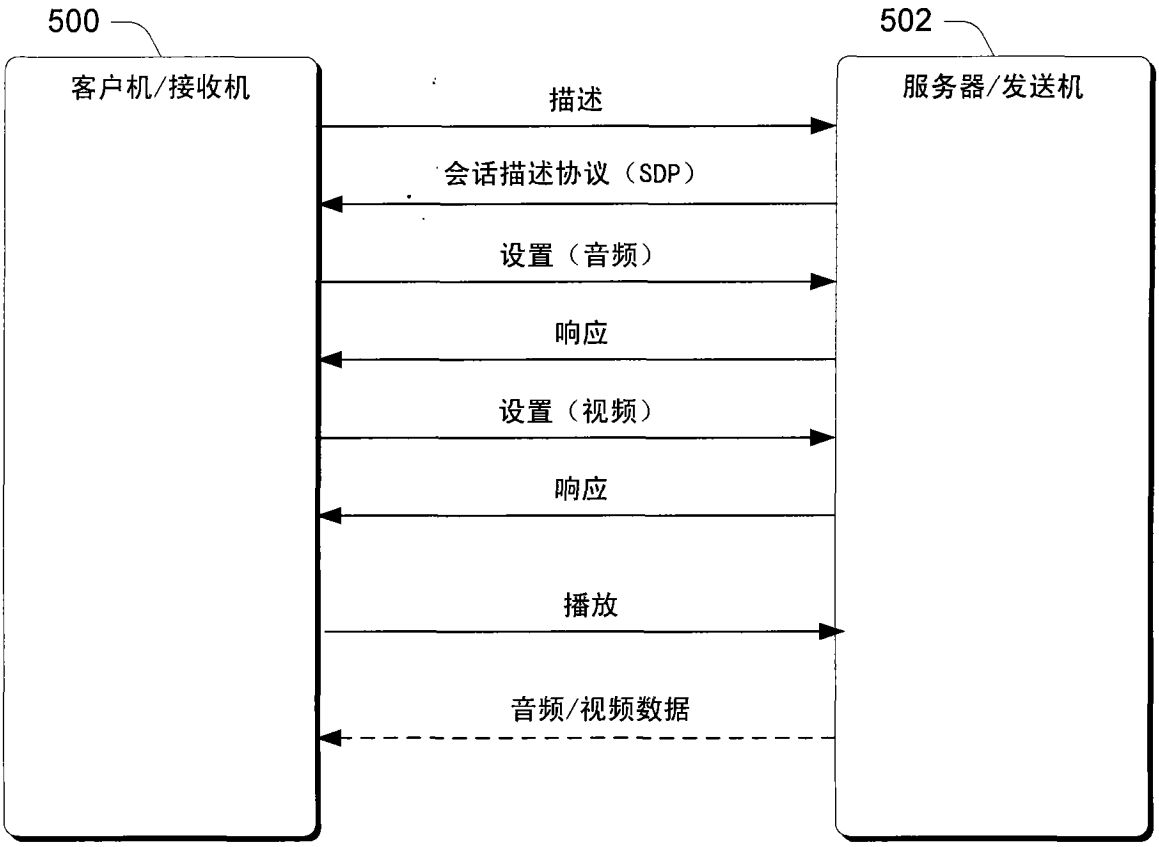


图 5

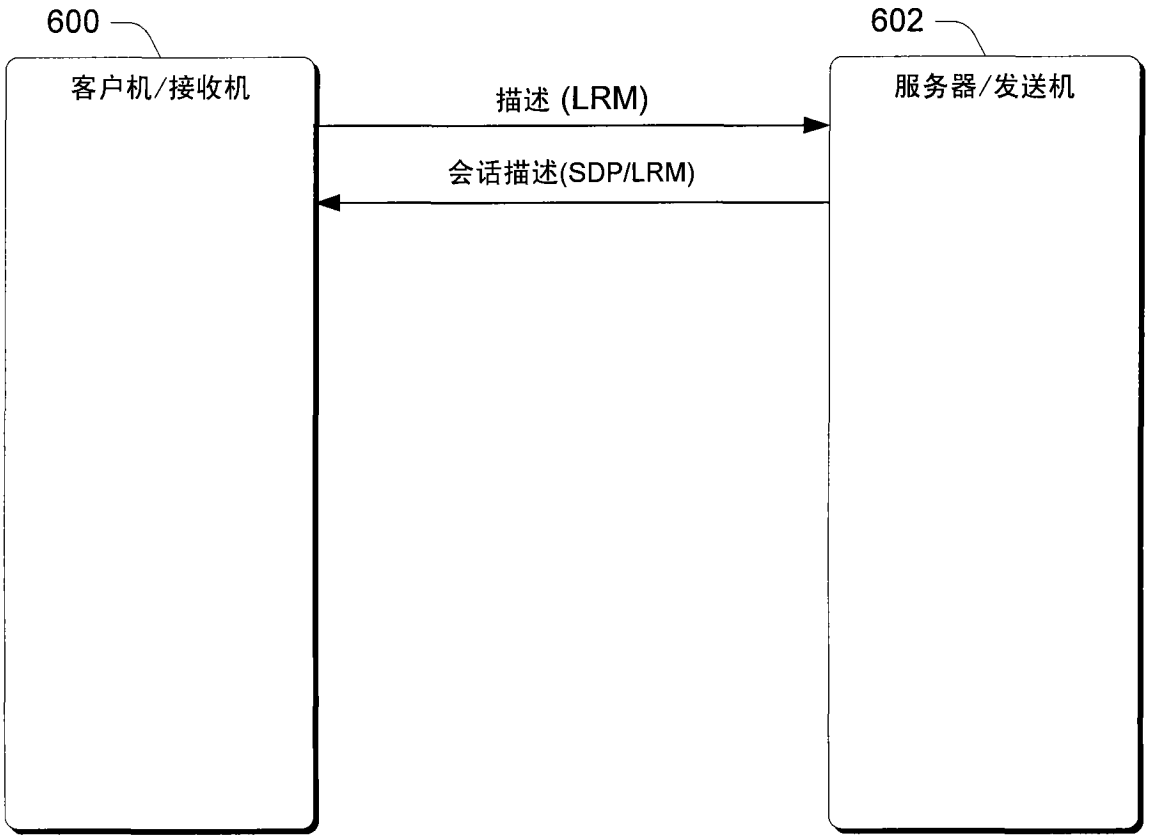


图 6

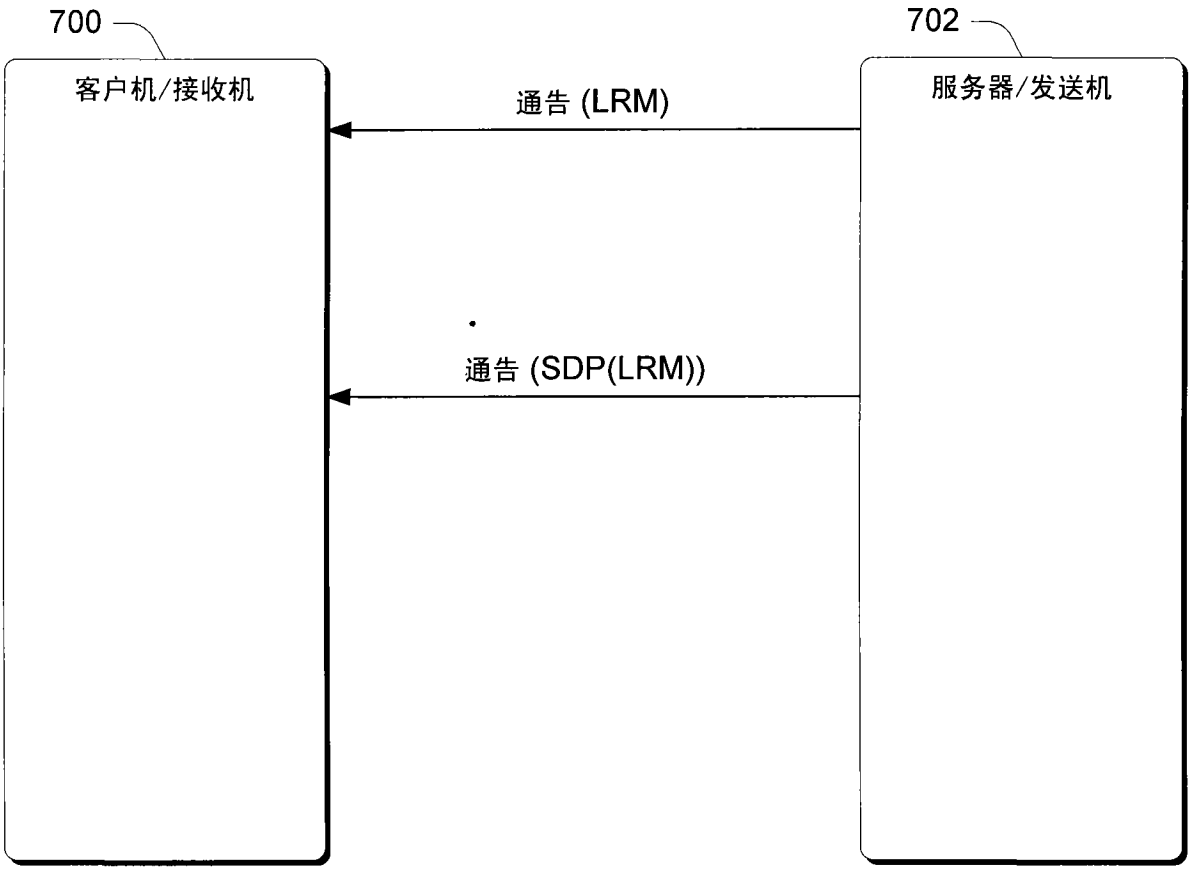


图 7

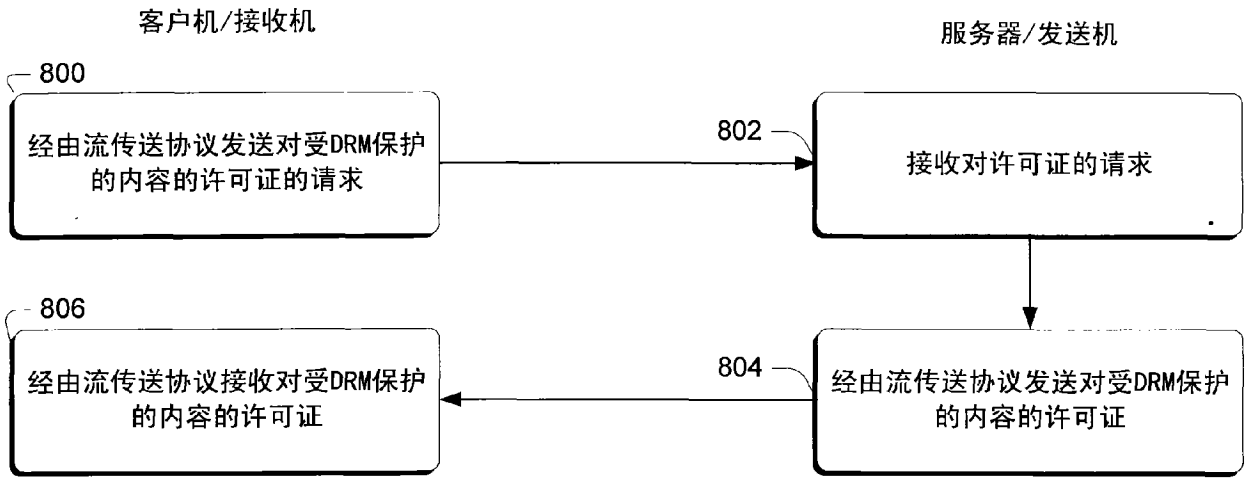

客户机/接收机
服务器/发送机
800
经由流传送协议发送对受DRM保护的内容的许可证的请求
802
接收对许可证的请求
806
经由流传送协议接收对受DRM保护的内容的许可证
804
经由流传送协议发送对受DRM保护的内容的许可证

图 8

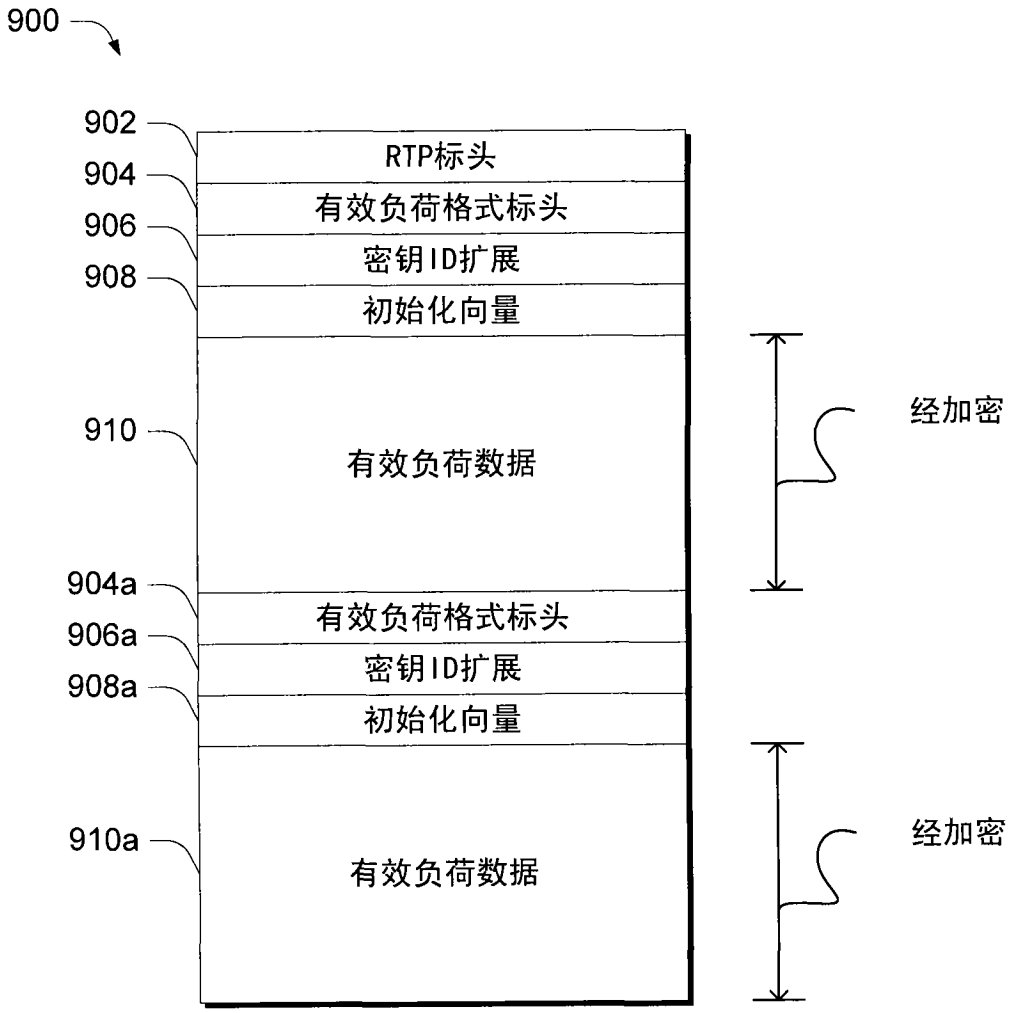

900
902
RTP标头
904
有效负荷格式标头
906
密钥ID扩展
908
初始化向量
910
有效负荷数据
经加密
904a
有效负荷格式标头
906a
密钥ID扩展
908a
初始化向量
910a
有效负荷数据
经加密

图 9

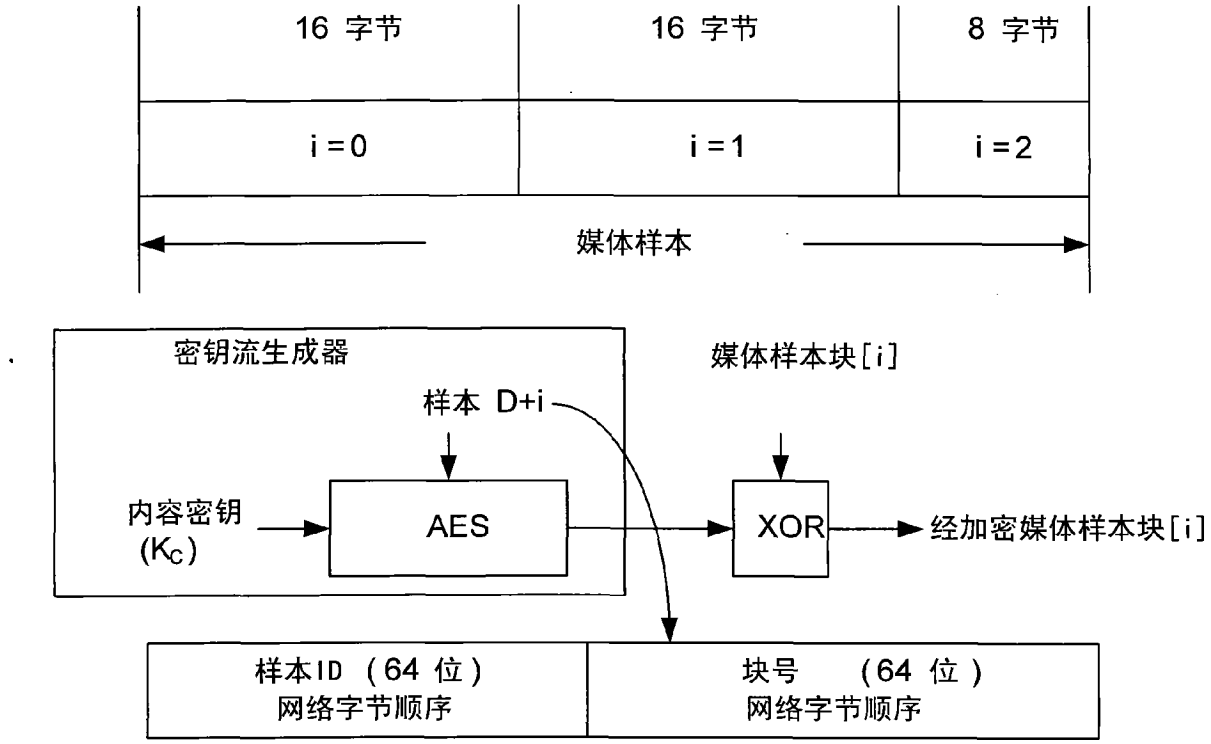

16 字节
16 字节
8 字节
i = 0
i = 1
i = 2
媒体样本
密钥流生成器
媒体样本块[i]
样本 D+i
内容密钥
(Kc)
AES
XOR
经加密媒体样本块[i]
样本ID （64 位）
网络字节顺序
块号 （64 位）
网络字节顺序

图 10

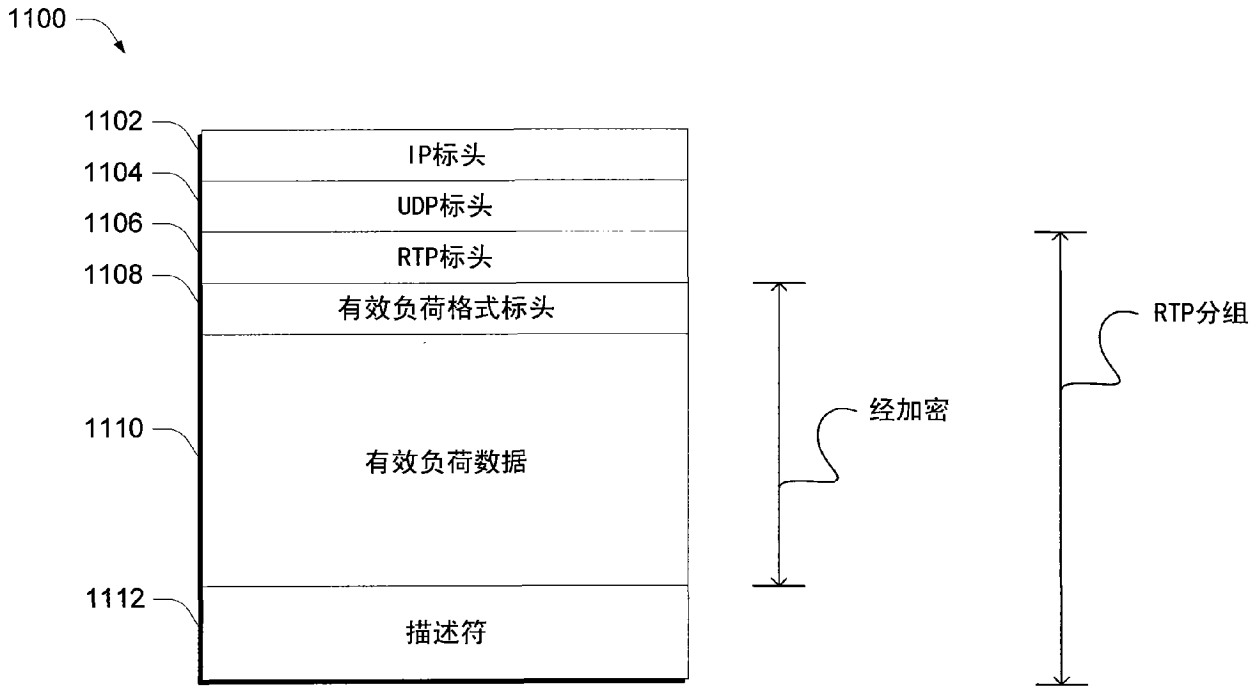

1100
1102
1104
1106
1108
1110
1112
IP标头
UDP标头
RTP标头
有效负荷格式标头
有效负荷数据
描述符
经加密
RTP分组

图 11