一种 P2P 环境下基于移动代理的 DRM 方案*)

李 平 卢正鼎 邹复好 肖尚勤
(华中科技大学计算机学院 武汉 430074)

摘 要 本文提出了一种 P2P 环境下的 DRM 方案。和传统的 DRM 方案相比,本方案具有 P2P 环境下数据分发速度快的优势,同时由内容提供者所委派的移动代理能代表其利益,完成权利的授予等 DRM 功能。本方案还支持权利的二次分发,从而激发了用户分发内容的积极性。分析表明,该方案安全可靠,并且易于实现。

关键词 数字版权管理,移动代理,P2P,认证中心

1 引言

近几年,P2P 技术发展迅速,并在互联网中得到广泛应用。同时 P2P 文件共享对数字版权的侵害也非常严重,因而在 P2P 环境下实现数字版权管理(DRM)变得非常紧迫[1]。DRM 中包括多种关键技术,其中权利转移(包括权利的迁移和二次分发)具有重要意义[2]。传统 DRM 系统大多基于 C/S 模式,并不适合 P2P 环境的特点;有人提出在移动手持设备上建立由硬件实现的可信平台模块,以实现 DRM 和权利的二次分发,但此方案对普通 PC 机并不适合[3];还有人提出在客户端引入本地 DRM 服务中心来实现二次分发,但该模式增加了客户端程序的复杂性和运行负担,同时存在一些安全隐患[4]。

针对这些情况,本文提出了一种 P2P 环境下基于移动代理的 DRM 方案。本方案中包括四个角色:认证中心、超级结点、内容提供者(即内容的权利所有者)和用户。认证中心可为内容提供者和用户颁发证书并提供证书的在线状态查询。用户从超级结点获得内容位置信息后,和内容提供者建立连接来获取加密内容。用户播放内容时,需要和内容提供者申请许可证。被授权代表内容提供者利益的移动代理到达用户,提供内容解密密钥并完成对用户的权利授予。而用户如果购买了二次分发权利,则可以将内容分发给其它用户,而相应收益由用户和原内容提供者共同分配。

本文的结构安排:首先介绍相关概念和原理;接着介绍各角色的主要功能和工作流程;然后分析了方案的性能及安全性,并与其它 DRM 方案进行了比较;最后引出本文的结论。

2 相关概念和原理

2.1 P2P(Peer to Peer)和数字版权管理 DRM (Digital Rights Management)

P2P 网络中每个结点的地位都是对等的。每个结点既可作为服务器为其它结点提供服务,又可作为客户来享用其它结点提供的服务。P2P 技术具有分布性、可扩展性、健壮性、负载均衡等特点。根据 P2P 网络拓扑结构,可将其划分为以下三种形式:

• 中心式拓扑:通过一个中心服务器来存放资源文件的索引和存放位置信息。优点是维护简单且查找效率高,不足之处是容易出现单点故障。代表软件是 Napster。

• 全分布式拓扑:没有专门的索引服务器,它采用了基于完全随机图的洪泛(flooding)发现和随机转发机制。该结构的可靠性好,但可扩展性较差。代表软件是 Gnutella。

• 半分布式拓扑:选择性能较好的结点作为超级结点(索引服务器),发现算法仅在超级结点之间转发。它综合了上述两种结构的优点,各项性能较均衡。代表软件是 KaZaA。

目前 P2P 软件在因特网上的应用非常广泛,影响巨大,例如使用 KaZaA 软件进行文件传输所耗费的带宽占了因特网总带宽的近 40%。而另一方面,P2P 文件共享的繁荣也为盗版提供了便利条件,内容提供者的权益受到了极大的侵害。P2P 的分布式特点又使得 DRM 的实现困难重重。因而寻找一种既能充分发挥 P2P 环境下文件分发的优越性能,又能有效保护内容提供者合法权利的 DRM 方案,是当前迫切需要解决的难点问题。

*)国家自然科学基金项目(60502024);湖北省自然科学基金项目(2005ABA267);信息产业部资助的电子信息产业发展基金项目(信部运[2004]479 号);科技部资助的科技型中小企业创新基金项目,04C26214201284。李 平 博士研究生,研究方向为 DRM,P2P,移动代理。

DRM 关键技术包括权利描述、权利转移和可信执行等。其中权利转移是指权利在设备间的转移(权利的迁移)和用户间的转移(权利的二次分发)。权利转移可以提高用户购买、使用内容的积极性,增强用户对 DRM 的接受度,又可以减少用户破解 DRM 系统的动机。

2.2 移动代理 MA(Mobile Agent)

MA 是一个代替用户或其它程序执行某种任务的程序,它在网络系统中从一个结点移动到另一个结点继续执行,并能够选择何时、向何地迁移,最后返回结果。它具有动态性和分布计算的特点。移动代理系统由 MA 和移动代理运行环境 MAE(mobile agent environment)组成。MA 可以从一个 MAE 迁移到另一个 MAE,与本地的服务/资源进行交互完成任务。

本方案中,与特制的移动手持设备不同,用户的 PC 上并不存在一个硬件的可信执行平台模块,因此将内容播放许可证(内含节目解密密钥和相关权利信息)交给用户端进行处理是不安全的,并难以保证内容提供者的合法利益。因此本方案由内容提供者派遣一个代表其利益的 MA,该 MA 到达用户端后,由它来完成权利的授予、内容的解密播放和其它相关 DRM 功能。通过比较派遣前和返回后 MA 的状态值,可以判断用户端是否对 MA 进行了非法操作(如试图获取内容解密密钥等),从而保证了 MA 的安全性。

2.3 公钥基础设施 PKI(Public Key Infrastructure)

PKI 技术[5]采用证书管理公钥,通过第三方可信任机构-认证中心 CA(Certificate Authority),把用户公钥和用户的其它标识信息(如名称、E-Mail 等)捆绑在一起,在因特网上验证用户的身份。PKI 是由公钥密码技术、数字证书、CA 和关于公钥的安全策略等部分共同组成的,它可以实现内容交易过程中的保密性、完整性、身份认证和授权、抗抵赖。

CA 是 PKI 的核心,其功能主要包括:证书发放、证书更新、证书撤销(发生于用户私钥泄漏、用户违规操作等情况)、证书验证。CA 管理 PKI 结构下所有用户(包括各种应用程序)的证书,负责被撤销证书黑名单的登记和发布,并提供在线的证书状态查询服务。

本方案中内容提供者和用户都需要在 CA 处申请并获取证书。在它们进行会话的初始阶段,双方需要交换证书,并到 CA 处查询对方证书的有效性以确认对方的身份。这样可以有效保证会话的安全性。

3 一种 P2P 下的基于移动代理的 DRM 系统方案

3.1 方案总体构架

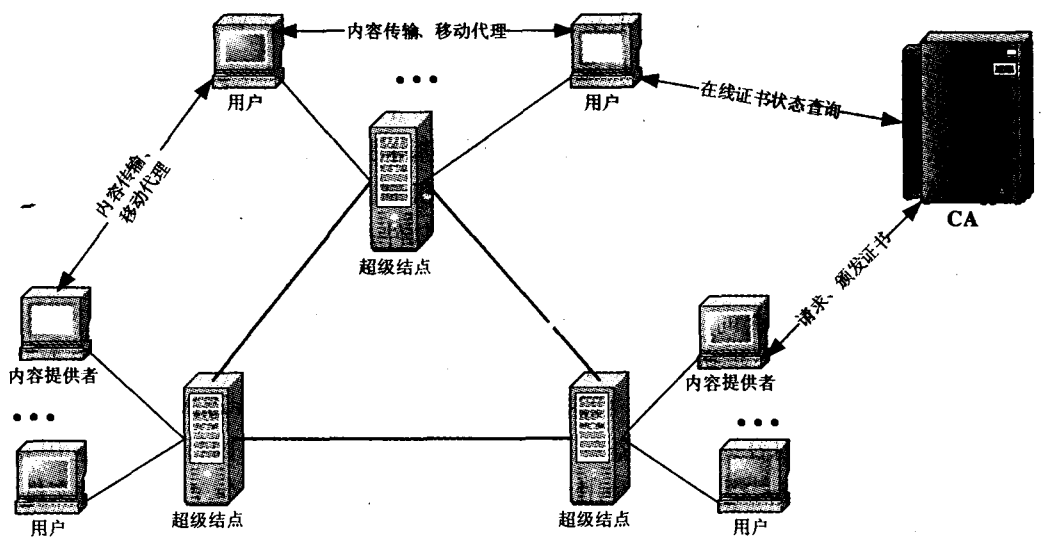

图 1 方案的总体结构图

本方案拓扑结构如图 1 所示(半分布式拓扑,类似于 KaZaA),方案中共包含四种角色:CA、超级结点、内容提供者和用户:

- CA 由专用的高性能服务器来承担,主要负责证书发放和在线证书状态查询服务。
- 超级结点由 P2P 网络下性能较好的机器来担当,提供内容索引和存放位置信息。
- 内容提供者可以由专用服务器或普通 PC 来实现,提供内容,并实现 DRM 功能。
- 用户是普通 PC,下载内容并付费观看。在购买二次分发权利后可成为内容提供者。

3.2 各角色的主要功能模块描述

各角色的功能模块较多,其中有不少是类似的,如注册模块、证书申请模块等。因此这里仅列出各

角色中最核心的功能模块。

1. CA

·注册模块：接受内容提供者和用户的注册请求，验证用户身份。

·证书生成模块：为通过验证的用户生成证书，证书应遵循 X.509 证书规范。

·证书发放模块：将证书以主动或被动的方式（放在网页上供用户下载）交付用户。

·证书撤销模块：撤销证书，将该作废证书的信息放入证书撤销列表中并发布。

·在线证书状态查询模块：为内容提供者和用户提供在线的证书状态查询。

2. 超级结点

·信息接收模块：接收内容提供者提交的内容索引和存放位置信息。

·信息维护模块：将信息分类整理并存储到数据库中；删除或修改信息。

·查询模块：接受用户内容查询请求，搜索本地数据库，若找到则向用户返回结果。

·信息搜寻模块：向相邻超级结点发出请求（信息不在本地）并返回最终结果给用户。

3. 内容提供者

·内容加密模块：将内容进行加密（如采用加密算法 AES）。

·证书状态查询模块：和 CA 会话，查询用户证书状态。

·内容传输模块：向用户传输加密后的内容。

·计费模块：根据用户情况（如普通用户和二次分发用户），收取相关费用。

·移动代理生成与派遣模块：接收用户许可证申请，生成并派遣移动代理。

·移动代理模块：在用户端和内容播放器交互，提供解密密钥以解密内容；写入用户端的权利文件；在用户间移动；携带相关信息返回。

·移动代理验证：比较移动代理派遣前和返回后的状态值，判断用户端有无违法操作。

4. 用户

·内容查询模块：从超级结点处获取所需内容的索引和存放位置信息。

·内容获取模块：建立会话，从内容提供者处获取内容。

·权利分析模块：分析权利文件，获知所拥有的内容权利。

·内容播放模块：和内容提供者派遣的移动代理交互，获取内容解密密钥，解密并播放内容（解密后的内容只能播放而不能存储到本地）。

3.3 系统工作流程

本方案中 DRM 的实现主要通过内容提供者和用户之间的交互来体现，因此这里重点描述它们之间的工作流程。此处的内容专指视频或音频资源。

a. 用户从内容提供者处获取内容

①用户和超级结点建立会话，获取所需内容的位置信息。

②用户和内容提供者建立会话，双方交换 CA 颁发的证书，并向 CA 查询对方证书的状态，若双方证书状态皆为有效则继续会话，否则中断会话。

③用户向内容提供者申请内容，内容提供者将加密后的内容传输给用户。

b. 用户申请内容播放许可证，内容提供者派遣 MA

①播放内容前，用户端的内容播放模块和内容提供者建立会话，申请内容播放许可证。

②用户和内容提供者交互，购买所需的内容权利，并缴纳相应费用。

③内容提供者根据本地存放的用户状态（如是否二次分发用户），生成相应 MA（记录其状态值）并派遣到用户端。MA 中携带用户购买的权利、内容解密密钥等重要信息。

④MA 到达用户端后开始运行，它和内容播放模块交互并提供内容解密密钥。内容播放模块使用该密钥解密内容并播放。

⑤MA 在用户端写入权利文件。用户可利用权利分析模块查看内容权利，但对该文件的修改（如增加权利）并不能获利，因为内容提供者将保存用户的权利信息并按该信息提供服务。

⑥MA 返回到内容提供者，内容提供者计算返回 MA 的状态值，并将该值与派遣前 MA 的状态值进行比较，以判断用户有无违规操作。

c. 用户二次分发内容

①若用户 A 购买了二次分发的权利，则可以通过向超级结点提供索引和位置信息来向其他用户提供该内容。注意内容仍保持原来加密后的形式。

②用户 B 从超级结点处获取到用户 A 的位置信息后，和用户 A 建立会话，交换证书，各自验证对方的身份。

③通过验证后，用户 B 从用户 A 处获取内容，并在播放前向用户 A 申请内容播放许可证。

④用户 B 和用户 A 交互，购买所需要的内容权利，并缴纳相应费用。

⑤用户 A 和原内容提供者建立会话，提交二次分发许可证请求，并将刚才所得费用的一部分付给内容提供者（如平均分配）。

⑥原内容提供者生成用户 A 新的权利文件并传输给用户 A，用户 A 用其覆盖原权利文件。

⑦原内容提供者生成 MA 并派遣到用户 B。MA 携带内容解密密钥和 B 的权利信息。

⑧MA 到达用户 B 后开始运行，提供密钥解密，写入权利文件。最后返回原内容提供者。

⑨原内容提供者检查 MA 的状态，判断用户 B 是否有违规操作。

此后用户 B 如有需要，将不再通过用户 A，而是直接和原内容提供者进行联系。

如果内容提供者发现用户有任何违规操作，可以采取相应措施来维护自身权利：(1)不再向该用户提供内容分发；(2)向 CA 提交该信息，CA 经确认后可考虑是否将该用户的证书作废。一旦证书作废，该用户将无法使用本方案提供的服务。

4 性能和安全性分析

4.1 性能分析

内容传输性能：本方案采用类似于 KaZaA 的半分布式 P2P 网络拓扑，用户从超级结点处获取内容存放位置信息后，将直接和内容提供者之间建立连接下载内容，不存在中心服务器瓶颈。而同时从内容提供者处下载该内容的用户数量越大，速度会越快。

移动代理效率：移动代理被设计为一个轻量级的程序，其功能简单，且携带的信息量不大(主要是解密密钥和权利信息)，因而能较快地在内容提供者和用户之间移动，效率较高。

4.2 安全性分析

角色安全性：通过引入 PKI 机制和 CA，内容提供者和用户可以利用证书确认对方身份，建立一个可信的通信环境(可在通信时使用安全套接层协议 SSL)。而对于有违规操作的用户，可以很方便地进行事后追究，如撤销证书等。

移动代理安全性：发出移动代理前，内容提供者记录移动代理的状态值，在移动代理从用户端运行完毕后返回时再次计算其状态值，比较两状态值可判断出用户是否有违规操作。

内容和权利信息的安全性：内容采用强加密算法 AES 进行加密，而加密的内容只能在专门的内容播放模块中进行解密播放，解密后的内容不能被存储。因而内容的安全可以得到保证；权利信息虽然在客户端以文件形式存储，但内容提供者是根据其本地存储的用户权利信息来进行处理的。因此即使用户篡改其权利文件也无法获利，从而保证了权利信息的安全性。

4.3 和其它 DRM 系统的比较

Srijith K. Nair 等人提出的 DRM 方案主要运用于移动手持设备，设备上有一个基于硬件的可信平台模块；而 S. H. Kwok 等人提出的方案需要在用户端建立一个本地 DRM 服务中心(数据库)来实现 DRM；这些方案都对客户端的硬件或软件有较高的要求，而本方案的实现对客户端要求较低，易于实现和推广。同时 CA 和 MA 的引入，增加了系统的安全性和灵活性，并有效保证了内容提供者的利益。

结论 本文提出了一种 P2P 环境下的基于移动代理的 DRM 方案。本方案具有 P2P 下文件分发速度快的优点，同时移动代理能较好地代表内容发布者的利益，实现 DRM 功能，并能较好地支持权利的二次分发。通过实验和分析表明，本方案具有较高的安全性且便于实现。

参 考 文 献

1 Iwata T, Abe T, Ueda K, Sunaga H. A DRM system suitable for P2P content delivery and the study on its implementation. In: Proceedings of The 9th Asia-Pacific Conference on Communications, APCC 2003, Sept. 2003, 2: 806～811

2 Dhamija R, Wallenberg F. A framework for evaluating digit rights management proposals. In: Proceedings of the 1st International Mobile IPR Workshop: Rights Management of Information Product s on t he Mobile Internet, Helsinki, Finland, 2003. 13～21

3 Srijith K, Nair, Popescn B C, Gamage C, Crispo B, Tanenbaum A S. Enabling DRM-preserving Digital Content Redistribution. E-Commerce Technology, 2005. CEC 2005. In: Seventh IEEE International Conference on July 2005. 151～158

4 Kwok S H, Lui S M. A license management model for peer to peer music sharing. International Journal of Information Technology and Decision Making, 2002, 1(3): 541～558

5 [美]Nash A, 等著. 张玉清, 等译. 公钥基础设施(PKI)实现和管理电子安全. 北京：清华大学出版社, 2002. 12～18