一个面向家庭网络的数字版权管理系统

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

摘 要 随着消费电子产品的普及,家庭网络逐渐流行,但与此同时网络上数字内容的侵权问题也非常严重。提出了一种对家庭网络内数字内容进行版权保护的数字版权管理(DRM)系统。系统中,家庭网关设备负责管理家庭网络内的所有用户电子设备,并作为它们的代理与外部DRM服务器交互,以执行DRM功能。系统采用的组密钥技术可使得经过加密的数字内容只有合法用户设备才能解密并使用,而通过数字内容在用户设备之间的超级分发可实现家庭网络内的内容共享。

关键词 数字版权管理,家庭网络,组密钥技术,RSA算法
中图法分类号 TP309 **文献标识码** A

Home Networks-oriented Digital Rights Management System

LI Ping LU Zheng-ding ZOU Fu-hao LING He-fei
(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract With the popularization of the consuming electronic products, home networks are prevailing gradually, at the same time the copyright infringement of the digital content in the network is very serious. A digital rights management (DRM) system for protecting the copyrights of digital contents in home networks was proposed. In the proposed system, the home gateway device is responsible for managing the user electronic terminals in the home network and interacting with the external DRM server to enforce DRM functions as their agent. The group key technique adopted by this system makes sure only the legal user terminals can decrypt the encrypted digital content and then consume, and the digital contents can be shared in the home network through the super distribution of the contents between the user terminals.

Keywords Digital rights management, Home network, Group key technique, RSA algorithm

1 引言

随着电子消费产品的普及以及无线通讯技术的成熟,与家庭网络有关的技术及标准已成为国内外关注和研究的热点。家庭网络是指通过家庭网关设备将公共网络功能和应用延伸到家庭,并以有线或无线网络连接各种信息终端,达到信息在家庭内网与外部公网的充分流通和共享[1]。用户可通过家庭网络享受诸如网络访问、IP电话、VOD点播、互动游戏等服务[2]。

与此同时,数字作品容易复制和传播的特点使得网络上数字作品的版权侵害行为非常严重[3],极大地损害了内容提供商的利益,阻碍了后者进一步提供服务和拓展市场。目前,解决该问题最主要的方法是采用DRM技术[4],不少公司还推出了自己的DRM系统产品。然而,家庭网络的独特之处使得目前的这些DRM系统对其并非完全适合。例如,在家庭网络内,用户一般都希望能在设备之间实现数字内容的方便共享,而大多数DRM系统对此并不支持。这样,即使某个数字内容已经存在于家庭网络内的一台用户设备上,当其它设备要使用该数字内容时,仍需要和DRM系统中的授权服务器发起连接,重新请求该内容的数字许可证,给家庭网络内的内容共享带来不便,并在一定程度上限制了DRM系统在家庭网络中的应用。

针对DRM系统中多个用户的内容共享问题,开放移动联盟(OMA)在其发布的DRM 2.0中提出了"域"(domain)的概念[5]。它指出,一个域中可以包括多个DRM代理,而授权服务器可以将权利和内容解密密钥绑定到这个域中的所有DRM代理上,因此这些DRM代理即使在离线的情况下也能进行数字内容的共享。一些研究者利用该思想,针对家庭网络应用环境提出了不同的DRM解决方案。例如,Lee Young Gu等人提出一种方案,其要点是在家庭网络中构建一个域,并在域中设置一个家庭授权域管理器(类似于家庭网关)来管理所有用户设备。此方案解决了数字内容在用户设备之间传

到稿日期:2008-12-14 返修日期:2009-03-03 本文受国家自然科学基金项目(60803112,60873226),国家信息产业部电子信息发展基金项目(信部运[2007]329号)资助。

李 平(1974-),男,博士研究生,主要研究方向为多媒体安全等,E-mail:lpshome@sina.com;卢正鼎(1944-),男,教授,博士生导师,主要研究方向为分布式系统集成、信息安全、数据库系统等;邹复好(1974-),男,博士,主要研究方向为多媒体安全等;凌贺飞(1976-),男,博士,副教授,主要研究方向为多媒体安全等。

输后数字许可证需要重新申请的问题，然而其管理模式较为复杂，对用户设备来说不够灵活[6]；Azfar Moid 等人则提出了一个基于 IEEE 802.1 用于家庭网络的系统结构，该结构可支持安全及可扩展的视频流传输，但其将研究侧重点放在移动设备上，且对用户设备的硬件要求比较高[7]。

通过上述分析，不难发现现有的 DRM 系统或关于家庭网络的 DRM 解决方案在权利管理模式、管理的灵活性等方面存在一些不足，因此本文拟提出一种新的基于组密钥技术的面向家庭网络的 DRM 系统，系统中家庭网关向因特网上 DRM 服务器申请的权利是基于家庭网络中所有合法用户设备的，该权利允许家庭网络所有合法注册的用户设备之间进行数字内容的共享，而系统所采用的组密钥技术则可以保证经过加密的数字内容只能被合法用户设备解密使用。此外，系统还支持用户设备之间通过数字内容的超级分发来实现内容的共享。

本文第 2 部分介绍系统总体结构、组密钥技术的基本原理及数字许可证的结构；第 3 部分描述所提出的 DRM 系统中各主要工作协议的细节；第 4 部分分析系统的性能和安全性，并和其它 DRM 系统及研究方案进行比较；最后给出结论。

2 系统结构与组密钥技术原理

2.1 系统总体结构

如图 1 所示，本系统中包含 3 种主要角色：家庭网关、用户设备和 DRM 服务器。

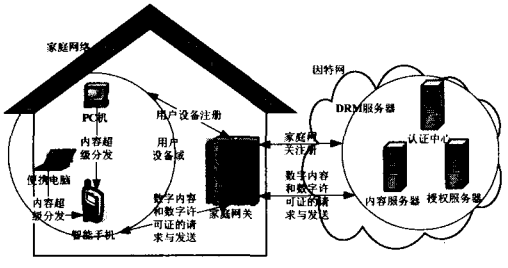

图 1 系统结构图

• 家庭网关：是家庭网络中的一个专用设备，可代理用户设备和 DRM 服务器交互获取数字内容和数字许可证，并管理家庭网络内所有用户设备。

• 用户设备：是家庭网络中的各类电子设备，包括 PC 机、便携电脑和智能手机等。

• DRM 服务器：位于外部因特网上，包括内容服务器、授权服务器、认证中心(CA)服务器等。其中内容服务器负责提供数字内容，授权服务器负责发布数字许可证，而 CA 服务器为家庭网关提供身份证书并提供证书的状态查询。这里，为突出家庭网络，将它们统一看作一个 DRM 服务器。

2.2 组密钥技术原理和数字许可证

系统中，家庭网关不仅是整个家庭网络与外部网络进行联系的桥梁，也是 DRM 系统得以实现的关键。下面简要介绍家庭网关对用户设备进行管理时采用的组密钥技术的原理。

1)当某用户设备希望加入家庭网络时，家庭网关首先验证该设备的相关信息，然后基于 RSA 算法为每个合法用户设备生成一对公钥和私钥。其中公钥用于生成组密钥和用户设备的身份证书，私钥用于解密数字许可证。

2)家庭网关使用所有合法设备的公钥来生成组密钥，并向 DRM 服务器提交该家庭网络的所有合法用户设备的列表和组密钥。DRM 服务器将根据该组密钥来加密内容解密密钥。

3)当家庭网关获得数字内容和数字许可证后，基于组密钥技术，所有合法用户设备都可以利用自己的私钥来解密内容解密密钥，并用它来解密数字内容并使用。

4)若某用户设备因为某种原因而从合法用户设备列表中被清除，则家庭网关将重新计算组密钥并将新的合法用户设备列表和组密钥提交给 DRM 服务器。此后该用户设备将无法继续使用系统提供的服务。

如图 2 所示，上面提到的数字许可证是一个用权利描述语言(如 ODRL 或 XrML)进行编写、用来描述数字内容权利使用信息的计算机文件，主要包含数字内容使用权利(包括使用权限、使用次数、使用期限和使用条件等)、数字许可证颁发者及其拥有者以及数字内容解密密钥(用户所获取的数字内容一般都是加密的，此内容解密密钥可用于解密数字内容)等信息。本系统中，家庭网关申请的数字许可证的拥有者是家庭网络内的所有合法用户设备，因此数字许可证中的内容解密密钥应该用家庭网关所提交的组密钥进行加密。这样，DRM 服务器针对某个数字内容，只需向家庭网关传输一次数字许可证，而家庭网络内的所有合法用户设备都可用自己的私钥来解密该数字许可证中的内容解密密钥，并最终解密数字内容。

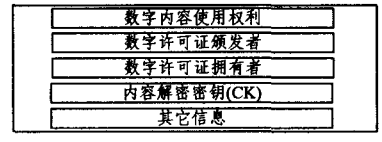

图 2 数字许可证的结构

3 DRM 系统的主要工作协议

3.1 用户设备的注册和移除

家庭网关负责管理家庭网络内的所有用户设备，用户设备在使用该系统的服务之前必须向家庭网关进行注册。

3.1.1 用户设备注册

①当一个新的用户设备希望加入家庭网络时，可以和家庭网关建立连接。

②家庭网关验证并记录用户设备提交的相关信息(如设备的 CPU 序列号、硬盘标识号等)，然后根据 RSA 算法按以下步骤为该设备产生公私钥对：

1)对于第 i 个用户设备，产生两个素数 p_i, q_i。可采用已有的素数测试算法，如 Miller Rabin 算法等。

2)计算 $N_i = p_i \times q_i$，这里 p_i, q_i 采用 256bit 的素数，p_i 和 q_i 过后将被丢弃以保证其不被获取。

3)计算 $\Phi(N_i) = (p_i - 1) \times (q_i - 1)$，并选择正整数 e 使得 e 与 $\Phi(N_i)$ 互质，即满足 $gcd(e, \Phi(N_i)) = 1$，e 作为公共参数公开。

4)计算 d_i，使其满足公式 $ed_i = 1 \bmod \Phi(N_i)$。将参数组合构成公钥 $K_i = \langle e, N_i \rangle$ 和私钥 $K_i^{-1} = \langle d_i, N_i \rangle$。

③用生成的公钥来产生用户设备身份证书，并将该证书及生成的私钥传输给该用户。

④家庭网关更新合法用户设备列表，并按下面方法生成(或更新)组密钥 GPK：首先取出所有合法用户设备 j 所拥有的公钥 N_j，$N_j \in S_r$(其中 j 为用户设备的序号，S_r 表示所有合法用户设备的公钥集合)，然后生成组密钥 GPK，这里 GPK=$\langle e, \prod_{N_j \in S_r} N_j \rangle$。

⑤每当有新的用户设备加入后，家庭网关会和 DRM 服务器连接，提交其更新的合法用户设备列表和组密钥。

3.1.2 用户设备移除

当家庭网关发现下列情况之一时，可将用户设备从其合法设备列表中移除：

①用户设备申请退出家庭网络；

②发现用户设备有版权侵害的行为。

当家庭网关移除该用户设备后，会更新其合法用户设备列表，并根据新的列表重新生成组密钥。同时，它会和 DRM 服务器连接，提交其更新的合法用户设备列表和组密钥。

3.2 家庭网关身份证书的管理

家庭网关在使用该系统的服务之前，必须向 DRM 服务器申请身份证书。以后每次和 DRM 服务器进行交互前，必须提供其身份证书，进行身份验证。

3.2.1 身份证书获取

①家庭网关和 DRM 服务器建立连接，提交其相关的设备信息和当前的合法用户设备列表。

②DRM 服务器对该信息进行审核。审核通过后，利用 RSA 算法为家庭网关生成公私钥对，公钥用于生成家庭网关身份证书，私钥用于解密数字许可证。

③DRM 服务器将该身份证书和私钥传输给家庭网关。

3.2.2 证书状态查询协议

通信实体(如家庭网关等)可向 DRM 服务器查询某个希望与其进行通信的其它实体的身份证书的状态，DRM 服务器会进行响应。

3.2.3 证书撤销

若 DRM 服务器发现家庭网络内的成员有版权侵害的行为(如采用数字水印等技术手段进行版权追踪)，经查实后可撤销该家庭网关的身份证书，这样该家庭网络将无法继续使用 DRM 服务器提供的服务。

3.3 数字内容和数字许可证的获取

当某用户设备需要数字内容时，由家庭网关代理它向 DRM 服务器请求该内容并执行相应 DRM 功能。具体工作协议的流程如图 3 所示。

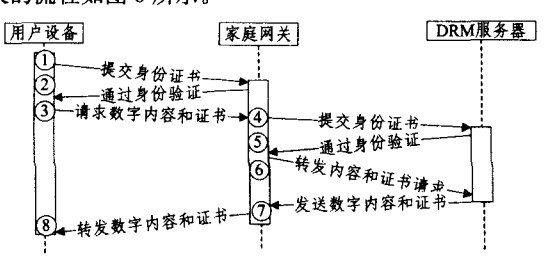

图 3 数字内容和数字许可证的获取协议流程

①当一台用户设备希望获取某个数字内容，可与家庭网关建立连接，提交其身份证书。

②家庭网关根据用户设备身份证书验证其身份的合法性。若通过验证，则继续下一步。

③用户设备向家庭网关请求数字内容和数字许可证。

④家庭网关和 DRM 服务器建立连接，提交其身份证书。

⑤DRM 服务器根据家庭网关的身份证书验证其身份的合法性。若通过验证，则继续下一步。

⑥家庭网关转发该用户设备的内容和证书请求。

⑦DRM 服务器根据其请求收取相应的费用，然后将其所需的数字内容和相应的数字许可证传输给家庭网关。

⑧家庭网关收到数字内容和数字许可证后，利用自己的私钥解密数字许可证，然后将证书和内容转发给该用户设备。

需要指出的是，DRM 服务器对要发布的数字许可证需进行两次加密。首先它用家庭网关提供的组密钥 GPK 对数字许可证中携带的内容解密密钥(假设为 CK)进行加密(可表示为 $E_{GPK}(CK)=CK^e \bmod \prod_{N_j \in S_r} N_j$)，然后使用家庭网关的公钥对整个数字许可证进行再次加密。

当家庭网关收到数字许可证后，首先用自己的私钥来解密该数字许可证，再将数字内容和解密的数字许可证转发给用户设备。用户设备可利用自己的私钥(假设为 K_j^{-1})来解密由组密钥加密的内容解密密钥，具体步骤如下：

$$\begin{aligned} D_{k_j^{-1}}(E_{GPK}(CK)) &= (CK^e \bmod \prod_{N_j \in S_r} N_j)^{d_j} \bmod N_j \\ &= (CK^e \bmod (N_j \cdot \prod_{t \in S_r \wedge t \neq j} N_t) \bmod N_j)^{d_j} \bmod N_j \\ &= (CK^e \bmod N_j)^{d_j} \bmod N_j \\ &= CK^{ed_j} \bmod N_j = CK^{x\Phi(N_j)+1} \bmod N_j \\ &= CK \end{aligned}$$

用户得到内容解密密钥后，可用它来解密数字内容并使用。需要强调的是，在用户设备端，数字内容的解密和使用由专门软件控制，可保证用户设备无法存储解密后的数字内容。

3.4 数字内容的超级分发

当用户设备(假设为 A)需要某个数字内容时，若该内容已经存在于家庭网络的其它一个用户设备(假设为 B)上，则 B 可以将该数字内容超级分发给 A，具体过程如下：

①A 和家庭网关进行连接并请求某个数字内容，若家庭网关发现该内容已经存在于 B 上，则它不必向 DRM 重新请求该内容，而是将信息告知 A。

②A 和 B 建立连接，提交自己的身份证书和内容请求。

③B 验证 A 的身份。若通过身份验证，则 B 可以将自己的数字内容、数字许可证超级分发给 A。

④A 可用自己的私钥解密数字许可证中的内容解密密钥，然后用该密钥解密数字内容并使用。

4 系统分析与比较

4.1 系统性能和安全性

系统中，家庭网关采用组密钥技术来管理所有用户设备，可实现对于某个数字内容，家庭网关只需要向 DRM 服务器请求一次该内容的数字许可证，而所有用户设备都可以使用该数字许可证来解密内容进行使用，这种方式减少了加密的运算量和数据的传输量。此外，在家庭网络内部，用户设备可以将其已获取的数字内容超级分发给需要它的其它用户设备，这不仅实现了设备之间内容的共享，也减轻了家庭网关的负担。

系统的安全性主要体现如下：

1)家庭网关和 DRM 服务器、家庭网关和用户设备以及

用户设备之间进行内容传输之前必须通过身份证书进行身份验证，保证了数据传输的安全性。

2)在本系统中，如果要解密数字内容进行使用，必须获取内容解密密钥，而内容解密密钥必须用用户设备的私钥来解密，因此数字内容加密方法的安全性等同于 RSA 算法的安全性。而对 RSA 算法最常用的攻击方式是分解 N_i，N_i 的位数越多，分解的难度就越大。这里 N_i 的位数为 512bit，足以保证系统的安全性。

3)实际使用的 DRM 系统常常采用某些方式进行版权的跟踪(如数字水印技术等)。如果家庭网关发现某用户设备有版权侵害行为，可将其从合法用户列表中清除；如果 DRM 服务器发现某家庭网络内的用户设备有版权侵害行为，可降低该家庭网络的信用等级，情况严重时可能会撤销该家庭网关的身份证书，使该家庭网络无法继续使用系统提供的服务。这种手段能够在很大程度上遏制数字版权侵害行为的发生。

4.2 与其它 DRM 系统的比较

微软公司的 WMRM(Windows Media Rights Manager)、Intertrust 公司的 DRM 系统以及本文所提出的 DRM 之间的比较如表 1 所列。

表 1 与现有的 DRM 系统的比较

	微软的 WMDM 系统	Intertrust 公司的 DRM 系统	本文所提出的系统
版权保护	能够实现	能够实现	能够实现
网络依赖	很高	非常高	较低
证书共享	不支持	不支持	支持

在版权保护方面，这 3 个 DRM 系统都能够实现对数字内容版权的保护，而本文提出的 DRM 系统主要侧重于保护家庭网络内的数字内容；在对网络的依赖性方面，由于微软的 WMDM 系统和 Intertrust 的 DRM 系统需要时刻保持在线连接以确保内容的安全性，因此对网络的依赖性很大，而本文提出的系统由于家庭网关设备的存在，使得 DRM 的大部分功能可以在本地完成，因此对网络的依赖性较低；在对数字许可证的共享方面，微软的 WMDM 系统和 Intertrust 的 DRM 系统都不支持，即每当内容重新传递后，都需要重新请求数字许可证，而本文提出的 DRM 系统则允许用户设备共享该内容的数字许可证。因此，相对现有的这些 DRM 系统来说，本系统更适合家庭网络这个特定的应用环境。

而通过和一些已提出的面向家庭网络的 DRM 研究方案相比(如前文所提到的 Lee Young Gu 等人及 Azfar Moid 等人提出的 DRM 方案)，本系统的管理模式更为灵活，通过组密钥技术和对内容超级分发的支持可方便地实现内容的共享，且对用户设备的硬件并无特殊要求，在实际环境中能得到较好的应用。

结束语 本文针对家庭网络的用户需求，提出了一种对家庭网络内的数字内容进行版权保护的 DRM 系统。系统中家庭网关通过组密钥技术，使得 DRM 服务器针对特定的数字内容只需传输一次数字许可证，并且只有合法用户设备才能使用该数字许可证。用户设备还可通过对数字内容进行超级分发来实现数字内容的共享。与已有的一些 DRM 系统相比，本系统的扩展性好，管理方式灵活，可方便地实现家庭网络用户设备之间数字内容的共享。

参 考 文 献

[1] 彭海清，冯涛，童登金. 家庭网络的关键技术、业务及标准化[J]. 研究与设计，2004(11)：5-8

[2] 房胜，钟玉琢. 蓝牙-家庭网络中服务的调用和实现[J]. 计算机科学，2004，31(2)：36-39

[3] Lin E T, Eskicioglu A M, Lagendijk R L, et al. Digital Video Content Protection[J]. Advances in Video Coding and Delivery, 2005, 93(1): 171-182

[4] Dhamija R, Wallenberg F. A framework for evaluating digit rights management proposals[C]// Proceedings of the 1st International Mobile IPR Workshop. Helsinki Finland, 2003

[5] Koster P, Montaner J, Koraichi N, et al. Introduction of the Domain issuer in OMA DRM[C]// The 4th Annual IEEE Consumer Communications and Networking Conference. Las Vegas NV USA, 2007

[6] Lee Young Gu , Lee Chang Bo . A Study on Secure Contents Transmission in Home Domain[C]// 2008 International Conference on Convergence and Hybrid Information Technology. Daejeon South Korea, 2008

[7] Moid A, Fapojuwo A O, Davies R J. Secure and Scalable Video Streaming over IEEE 802. 11e based Home Networks[C]// 2007 Canadian Conference on Electrical and Computer Engineering. Vancouver BC Canada, 2007

(上接第 105 页)

[5] Caronni G, Waldvogel M, Sun D. Efficient security for large and dynamic multicast groups[C]// Stanford. Proc the 7th Workshop on Enabling Technologies (WETICE'98). Washington: IEEE Computer Society Press, 1998: 376-383

[6] Wong C K, Gouda M, Lam S S. Secure group communications using key graphs[J]. IEEE/ACM Trans. Networking, 2000, 8(1): 16-30

[7] Kwak Deuk-whee, Kim Jong won. A Decentralized Group Key Management Scheme for the Decentralized P2P Environment [J]. IEEE Communications Letters, 2007, 11(6): 555-557

[8] Duta R, Barua R. Provably Secure Constant Round Contributory Group Key Agreement in Dynamic Setting[J]. IEEE Transactions on Informations Theory, 2008, 54(5): 2007-2025

[9] Song Ronggong, Korba L, Yee G O M. A Scalable Group Key Management Protocol[J]. IEEE Communication Letters, 2008, 12(7): 541-543

[10] Wu T C. Remote Login Authentication Scheme Based on a Geometric Approach[J]. Computer Communications, 1995, 18(12): 959-963

[11] Hwang M S. Cryptanalysis of a Remote Login Authentication Scheme[J]. Computer Communications, 1999, 22(8): 742-744

[12] Chien H Y, Jan J K, Tseng Y M. A Modified Remote Login Authentication Scheme Based on Geometric Approach[J]. Journal of Systems and Software, 2001, 55(3): 287-290

[13] Wang S J. Yet another login authentication using N-dimensional construction based on circle property[J]. IEEE Trans. on Consumer Electronics, 2003, 49(2): 337-341

[14] Wang S H, Feng B, Wang J. Comments on Yet Another Log-in Authentication Using N-dimensional Construction [J]. IEEE Transaction on Consumer Electronics, 2004, 50(2): 606-608

[15] Yang F Y, Jan J K. Cryptanalysis of Log - in Authentication Based on Circle Property [J]. IEEE Transaction on Consumer Electronics, 2004, 50(2): 625-628

[16] Wu T C, He W-H. A geometric approach for sharing secrets[J]. Computer & Security, 1995: 135-145

[17] Chor L P , Jing H W , Chong T P . A geometric approach for shared secrets, a refinement[J]. Computers & Security, 1998, 17(10): 725-732