多媒体社交网络中的数字内容安全分发研究

张志勇 杨丽君 黄 涛
(河南科技大学电子信息工程学院 洛阳 471003)

摘 要 多媒体社交网络(Multimedia Social Networks,MSN)的出现与快速发展,使用户间的信息交换与共享变得更加便利,而随意分发受版权法律保护的数字内容的现象也愈演愈烈。这种开放式网络环境下的数字版权管理(Digital Rights Management,DRM)问题已成为目前的一个开放问题和重要挑战。针对社交网络用户节点间的数字内容共享与传播行为,并基于支持可信验证代理方的远程证明,提出了多媒体社交网络环境下的数字内容分发体系框架及其安全协议。与现有典型DRM方案的对比分析表明,新方案结合可信计算高安全性的用户终端平台,实现了安全增强、可信、可控的数字版权保护机制,从而满足了用户终端平台的隐私保护需求。

关键词 多媒体社交网络,数字版权管理,远程证明,数字内容分发,安全协议
中图法分类号 TP309 **文献标识码** A

Research on Secure Distributions for Digital Contents in Multimedia Social Networks

ZHANG Zhi-yong YANG Li-jun HUANG Tao
(Electronic Information Engineering College, Henan University of Science and Technology, Luoyang 471003, China)

Abstract The emerging and rapid development of Multimedia Social Networks make information changes and shares among users much more convenient, but the phenomenon of unauthorized distributions on copyrighted digital contents becomes more serious. Digital rights management is an open issue and key challenges in the open network. With regard to behaviors of digital contents share and dissemination among social network user nodes, a framework and its secure protocol for digital contents distribution were proposed based on a trusted attestation proxy party-enabling remote attestation in MSN. The proposed DRM scheme was analyzed and compared with the typical ones available, and the results denote that combined with the trusted computing-supported high-level security user terminals, the novel method implements enhanced security, trustworthy and controllable mechanism on digital copyrights protection, and meets the requirement for platform privacy protections.

Keywords Multimedia social network, Digital rights management, Remote attestation, Digital contents distribution, Security protocol

1 引言

多媒体社交网络(Multimedia Social Networks,MSN)旨在为社会网络下同一(或不同)群组之间的用户提供多媒体信息交换与共享的网络工具、服务及应用。与传统客户/服务器模式的开放网络相比,MSN具有分布式特征以及直接、快速、灵活的音视频数字内容信息传输优势,因此在多媒体通信网络的建立和数字内容大范围传播方面提供了一个强有力的基础设施平台。然而,这种开放式多媒体网络环境所提供的信息交换与交互的便利,加之数字内容具有无损复制、易于分发的重要特性,使数字版权管理(Digital Rights Management,DRM)问题更加凸显出来,成为新的开放问题与挑战。数字内容非法拷贝、随意分发和传播等侵权现象变得越来越普遍[1]。通过DRM技术手段,在完整的数字内容价值链及其生命周期内(包括数字内容生成、分发、传输、使用和分享),对数字内容的知识产权进行保护,确保其合法、合理使用和可控传播[2]。此外,近年来可信计算技术的产生与发展,为DRM数字内容的安全分发以及用户高安全性终端平台上的数字内容使用控制提供了可行性和互操作性[3]。

本文结合可信计算中的远程证明关键技术[4],针对多媒体社交网络下的用户节点间多媒体内容分发和共享行为,提出了基于远程证明的数字内容安全分发方案,实现了有效的数字版权保护机制,从而满足了用户终端平台的隐私保护需求。

2 相关研究工作

2.1 社交网络

社交网络又称社会网络或人际网络,是由某些特定群体

到稿日期:2011-05-21 返修日期:2011-09-18 本文受国家自然科学基金项目(61003234),中国博士后科学基金资助项目(20100471611),河南省高等学校科技创新人才计划基金项目(2011HASTIT015),河南科技大学博士科学研究基金(09001470)资助。

张志勇(1975—),男,博士(后),副教授,CCF高级会员,主要研究方向为数字版权管理、可信计算与访问控制,E-mail:z.zhang@ieee.org;杨丽君(1988—),女,硕士生,主要研究方向为数字版权管理与多媒体社交网络;黄 涛(1966—),男,硕士,实验师,主要研究方向为数字版权管理与使用控制。

之间按照某种关系连接在一起而构成的相对稳定的关系网络。这些群体可以是个人、组织、企业甚至国家，他们之间的关系可以是朋友、同事、外交关系等。社交网络关注的是人们之间的互动与联系。基于社交网络的一个著名研究是1967年Stanley Milgram的连锁信实验和六度分隔理论(Six Degrees of Separation)，它揭示了社交网络尽管复杂但具有小世界特性。小世界网络(Small-world Network，SWN)最重要的特征是具有较短的平均路径长度和较高的聚集系数。社交网络一般由节点和边构成。节点表示社交网络中的行为主体，即个人、组织或智能体(Agent)；边则表示节点之间的联系，它是基于用户之间的某些特定关系，如朋友关系、业务关系或组织关系等而建立的。如图1所示，社交网络中用户之间通过某种特定关系组成各自的小世界网络(如SWN 1、SWN 2等)，用户之间在建立了某种关系的基础上，便可实时地进行信息交换与资源共享。

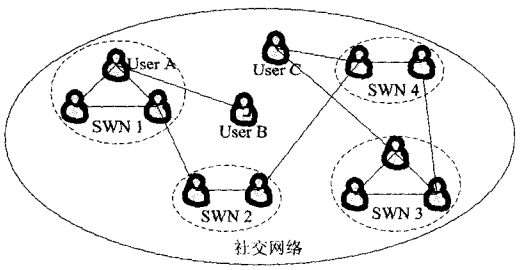

图1 社交网络基本结构图

2.2 远程证明技术

可信计算组织(Trusted Computing Group，TCG)用实体行为的预期性来定义可信：如果一个实体的行为总是以预期的方式达到预期的目标，那么这个实体就是可信的。TCG组织提出的可信远程证明方案是在计算机硬件平台上引入安全芯片架构，通过提供的安全特性来提高终端系统的安全性。其核心是通过可信平台模块(Trusted Platform Module，TPM)提供的度量机制，使计算机系统可以TPM为信任根，通过信任传递，将信任延伸到整个计算机系统。它的基本原理是可信计算平台对系统平台配置做全面的度量，度量结果保存在平台配置寄存器(Platform Configuration Register，PCR)中，系统平台通过这些度量过的信息向远程通信方证明自身运行环境是安全可信的。由于PCR中存放的测量结果由底层硬件安全模块保证其不可随意更改，因此度量结果是可信的，从而可以认为在度量结果是安全状态的计算环境下产生的计算结果便是可信的。

作为可信计算中的关键技术，远程证明(Remote Attestation，RA)[5,6]则是发出证明请求的一方确认远程平台的身份、平台状态配置信息及平台运行环境(动态)是否可信的过程。它使得证明请求方可以检测到被证明的计算机的变化，这样可以避免向不安全或安全受损的计算机发送私有信息或重要命令。

目前，国内外对RA的研究主要集中在度量方式和验证机制上。现有的比较典型的RA模型有基于二进制代码度量的TCG方案(BBRA)、基于属性的证明(PBRA)、卡内基梅隆大学的基于软件的远程证明(SWATT)及基于语义的远程证明(SBRA)等。远程证明的典型交互模型大致可分为4类，即直接证明模型、“拉”式证明模型、“推”式证明模型及基于第三方代理的证明模型。

2.3 AP²RA模型

现有远程证明模型的不足之处在于暴露了用户终端平台(包括硬件和软件)的基本配置信息，不能有效地保护终端平台隐私，而这正是MSN环境下一般节点用户的基本需求以及DRM技术可接受性的重要体现。因此，在如何有效地实施远程证明的同时，保护终端平台的隐私信息，对于多媒体社交网络环境下的数字内容安全分发，显得尤为重要。

文献[7]提出了支持验证代理方的远程证明模型(AP²RA)，如图2所示。AP²RA模型通过引入可信第三方——验证代理方(Attestation Proxy Party，APP)改进现有的远程证明模型，由APP验证组件来验证平台的完整性和安全性，并以RA报告的形式发送给验证方。这里验证方并未得到被验证方的平台配置细节和安全属性特征，有效地解决了被验证方的平台隐私保护问题，同时提高了验证系统的可生存性。一旦验证方被攻陷，APP仍然可以有效地提供远程证明服务，并安全地保持验证的结果。

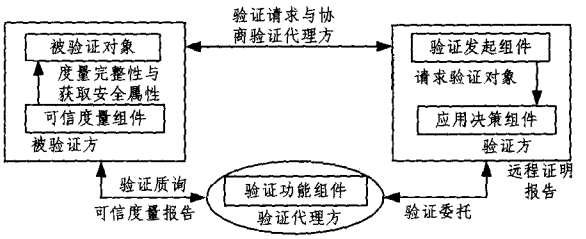

图2 支持验证代理方的远程证明模型[7]

3 多媒体社交网络下基于远程证明的数字内容分享

传统的DRM技术主要是针对数字内容全生命周期内的版权保护问题，而多媒体社交网络下DRM的研究重点集中于节点用户间的数字内容分发与共享。在这种开放式网络环境下，数字内容更易被随意分发、恶意传播和非法扩散。要保证用户间能够安全、可信、可控地交换数字内容，并有效地保护用户及其终端平台的隐私，就需要一个有硬件安全支撑、防拷贝和防篡改的可信计算用户终端环境，以及基于远程证明的数字内容分发模式和安全机制。

3.1 基于AP²RA的数字内容分发体系框架

图3描述了多媒体社交网络中两个用户(图1中的User A和User B)之间基于AP²RA的数字内容分发体系框架。该框架包括内容分发商、数字权利与证书分发商、两个终端用户平台(User A和User B)、验证代理服务器(APP)、完整性度量值与安全策略参考数据库，以及可信度量日志(Trusted Measurement Logging，TML)。其中，内容分发商可通过“拉”和/或“推”模式向终端用户分发数字内容；数字权利与证书分发商同样可采用“拉”和/或“推”模式向数字内容用户终端分发数字权利(许可证)，并作为CA(Certificate Authority)向终端和APP发放身份认证证书；两个终端用户平台即是支持可信计算的用户终端设备；验证代理服务器是远程证明过程的施动者，用来验证双方平台身份的可信第三方；完整性度量值与安全策略参考数据库用于存放由设备生产商提供的平台设备完整性度量值与安全策略值，作为APP对平台验证的参考标准值；可信度量日志TML用于存放终端用户平台本地完整性度量及获取安全属性的整个过程。

这里假定：

(1)对于数字内容分享的终端用户(User A和User B)平

台，确保配置是支持可信计算的高安全终端设备；

(2)该框架将 DRM 中数字权利(Digital Rights)提供方和身份认证中心(CA)所完成的功能，合并为数字权利与证书分发商；

(3)User A 合法地从内容分发商得到受版权保护的数字内容，并由 User A 向 User B 分享或分发数字内容。

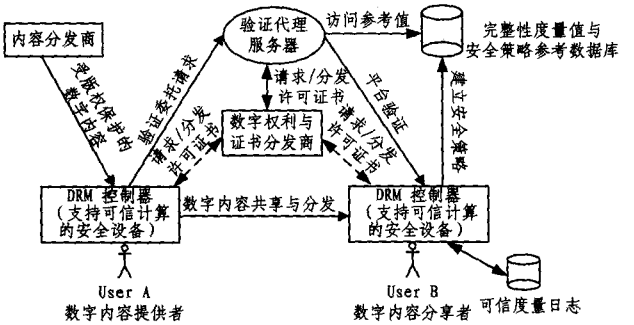

图 3 基于 AP²RA 的数字内容分发体系框架

3.2 基于远程证明的内容分发安全协议

基于图 3 描述的框架，该远程证明协议中包含 3 个实体：User A、User B、APP，分别对应 AP²RA 中的验证方、被验证方、验证代理方，AO 为被验证对象。协议中所涉及到的签名算法可采用基于公钥密码体制的 RSA、ECC 算法等，散列算法可采用 SHA-1、MD5 算法等。在开始 RA 会话前，假定 User A、User B 及 APP 已从数字权利与证书分发商获得了验证身份密钥 AIK 证书，K(APP-User A)和 K(APP-User B)分别为 APP 和 User A、User B 之间在 RA 会话开始前产生的共享秘密密钥。该远程证明安全协议时序图及具体消息交互如图 4 所示。协议过程如下：

(1)首先是 User B(数字内容分享者)向 User A(数字内容提供者)发出数字内容共享与访问请求；

(2)收到请求，User A 验证 User B 平台身份，准备代理协商；

(3)确认 User B 平台身份后，双方进行 APP 协商，最终确定一个进行平台验证的代理服务，并由它保护 User B 平台的隐私；

(4)若协商失败，则该协议终止；若协商成功，User A 向 APP 发出一个验证代理请求，发送的消息内容包括 AIK 私钥签名的被验证对象名称 Signature(AO_Names，SK(User A. AIK))、被验证对象的名称、AIK 证书 Cert(User A. AIK)，以及一个本地生成的随机数 Nonce；

(5)APP 收到消息内容后，通过 APP. AIK 证书验证 User A 的平台身份并获得 AO，进而决定接受或拒绝 User A 的验证委托；

(6)发送委托结果：若 APP 接受委托，协议继续执行，否则协议终止；

(7)APP 向 User B 发出对 AO 的 RA 质询消息，其中包含第(4)步中本地所生成的随机数 Nonce；

(8)User B 对多个 AO 进行本地完整性度量，其度量散列值和相应的度量顺序存放在 PCRs 中，此外还获得 AO 的安全属性特征值 secureAttributes，将此过程写入可信度量日志中；

(9)User B 使用平台验证身份证书 AIK 的私钥 SK(User B. AIK)对 PCRs 与包含有平台标识值(如可信芯片模块标识码)的 TML 等内容进行签名，并将其与 PCRs、secureAttributes、User B. AIK 证书和 TML 一起作为应答消息通过安全信道发给 APP；

(10)APP 收到 RA 质询应答后，首先结合数字权利与证书分发商判定 Cert(User B. AIK)的有效性，其次通过询问完整性度量参考值数据库，验证平台当前的完整性，同时结合事先在数据库中建立的安全策略，验证平台(包括 OS、关键组件及系统安全等级等)的安全配置；

(11)APP 证明 User B 平台后，通过安全信道将描述平台完整性与对象安全性状态及其签名值，连同 APP 公钥证书 Cert(APP. AIK)一起作为 RA 报告，发送给 User A；

(12)User A 基于 APP 的 RA 报告，作出访问决策；

(13)向 User B 共享或拒绝访问数字内容。

该协议第(11)步中的 RA 报告不使用证书机制将验证结果返回 APP，虽然证书在有效期内可多次使用，但鉴于平台软硬件的更新和基本安全策略的变化，APP 验证结果仅对激活本次协议的应用会话有效，再次应用会话需重新执行协议。

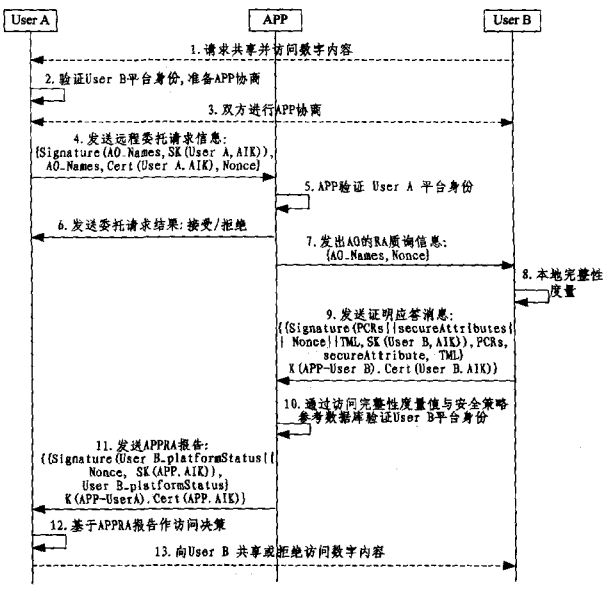

图 4 基于远程证明的数字内容分享安全协议时序图

3.3 方案对比分析

将本文提出的方案与现有的代表性方案，如 OMA DRM、文献[8]的“授权域”(Authorized Domain)、文献[9]的 LDM(Local Domain Manager)和文献[10]的 CPSec DRM 系统，在功能性、安全机制、系统开销等方面进行了对比，如表 1 所列。

表 1 相关方案的功能性与安全机制对比

功能性与安全机制	OMA	文献[8]	文献[9]	文献[10]	本文
数字内容安全分发	内容加密	内容加密	内容加密	内容加密	AP²RA 远程证明
数字许可分发机制	基于一般安全域	授权域	LDM 和代理证书	基于用户许可证	AP²RA 远程证明
密码方法	PKI	对称密码	PKI	非对称密码	PKI
用户终端	普通	普通	普通	普通	可信计算平台
版权保护机制	许可授权	许可授权与转移	许可授权与安转移	时空约束	远程证明安全增强
系统开销	适中	较少	较大	适中	较大
适合场景	普通安全域	数字家庭网络	数字家庭网络	普通网络应用	一般开放网络

上述典型方案和本文方案均实现了数字内容及其相应许可的安全分发，前者主要采用传统的数字内容加密方法，而本文则基于 AP^2RA 远程证明方法，结合可信计算用户终端平台实现多媒体内容的安全、可信分发；在系统开销上，本文方案采用了第三方可信平台验证机制，因此开销略大，但更适合于一般开放网络。

结束语 为解决多媒体社交网络应用下的数字内容版权管理问题，本文将可信计算中的远程证明技术引入到 DRM 安全方案中，提出了一种基于支持验证方代理的数字内容分发方案与安全协议。通过与其他代表性的 DRM 方案相比，本文方案提高了数字内容分享和传播的安全性、可信性和可控性，从而满足了 MSN 中用户节点终端平台的隐私保护这一实际需求。进一步工作将对本文协议进行形式化验证分析，并将其应用于普适的社交网络信息交换与共享应用服务中。

参 考 文 献

[1] Rosenblum D. What anyone can know: The privacy risks of social networking sites [J]. IEEE Security and Privacy, 2007, 5 (3): 40-49

[2] 张志勇，牛丹梅. 数字版权管理中数字权利使用控制研究进展[J]. 计算机科学，2011，38(4)：48-54

[3] 邱罡，王玉磊，周利华，等. 基于可信计算的 DRM 互操作研究[J]. 计算机科学，2009，36(1)：77-80

[4] Grawrock D. TCG Specification Architecture Overview Revision 1. 4 [EB/OL]. https://www. trustedcomputionggroup. org/groups/ TCG_1. 4_Archiecture_Overview. pdf, 2011-05-01

[5] 谭良，刘震，周明天. TCG 架构下的证明问题研究及进展[J]. 电子学报，2010(5)：1105-1112

[6] 张焕国，陈璐，张立强. 可信网络连接研究 [J]. 计算机学报，2010，33(4)：706-717

[7] 张志勇，裴庆祺，等. 支持验证代理方的远程证明模型及其安全协议[J]. 西安电子科技大学报，2009，36(1)：58-63，105

[8] Popescu B, Crisop B, Tanenbaum A, et al. A DRM security architecture for home networks [C] // Proceedings of 4th ACM Workshop on Digital Rights Management. Oct. 2004

[9] Kim H, Lee Y, Chung B, et al. Digital Rights Management with right delegation for home networks [C] // Proceedings of 9th International Conference on Information Security and Cryptology. LNCS 4296, 2006: 233-245

[10] 马兆丰，范科峰，陈铭，等. 支持时空约束的可信数字版权管理安全许可协议[J]. 通信学报，2008，29(10)：153-164

(上接第 62 页)

[4] Lee W, Stolfo S J. A Data mining framework for building intrusion detection models [M]. IEEE Computer Society Press, 1999: 120-132

[5] Yue Yao-xue. The Research of Network Intrusion System Based on Algorithm of Data Mining[J]. Comput-er Security, 2009, 10: 41-43

[6] Liu He-bing, Shang Jun-ping. On Clustering Analysis Algorithm [J]. Journal of Yiyuan Vocational and Technical Collage, 2006, 5 (4): 4-7

[7] Hartigan J A, Wong M A. A K-Means Clustering Algorithm [J]. Journal of the Royal Statistical Society, Series C (Applied Statistics), 1979, 28(1): 100-108

[8] Xindong W, Kumar V, Quinlan J R, et al. Top 10 Algorithms in Data Mining[J]. Knowledge and Information Systems, 2008, 14 (1): 1-37

[9] Li Ling-juan, Li Bing, Xue Ming. Research on Application of K-MEANS Algorithm in IDS[J]. Computer Technology and Development, 2010, 20(7): 129-131

[10] Fukunaga K, Narendra P M. A Branch and Bound Algorithm for Computing K-Nearest Neighbors [J]. IEEE Transactions on Computers, 1975(7): 750-753

[11] Li Yang, Fang Bin-xing, Guo Li, et al. A Network Anomaly Detection Method Based on Transduction Scheme[J]. Journal of Software, 2007, 18(10): 2595-2604

(上接第 78 页)

结束语 本文主要针对物联网环境中的服务获取问题提出了一种基于人工能量势的空间社区服务获取方法。物联网中的节点在进行服务获取时，利用节点最大有效传输范围选择下一跳节点，提高了节点生存周期，也在一定程度上增强了服务获取的效率。但是由于空间社区中节点的多样性和海量性，导致在一定程度上影响到服务获取的安全性和发现效率，我们下一步工作将集中于如何构建物联网实验床并开发基于人工能量势的服务获取原型系统。

参 考 文 献

[1] Commission of the European Communities. Internet of Things-An Action Plan for Europe (1st Edition) [R]. Brussels: COM, 2009, 278: 1-12

[2] Yu Tao, Zhang Yue, Lin K-J. Efficient Algorithms for Web Services Selection with End-to-End QoS Constraints[J]. ACM Transactions on the Web, 2007, 1(1)

[3] 王杨，王汝传. 一种基于 Echord 协议的网格资源发现方法[J]. 电子学报，2010，38(11)：2499-2504

[4] Zhao Q, Liu J, Xu J. Improving Search on Gnutella-like P2P Systems [C] // Computational Science-ICCS2007-7th International Conference. Berlin Heidelberg: Springer-Verlag, 2007, 4490(4): 887-890

[5] Khatib O. Real-time obstacle avoidance for manipulators and mobile robots [J]. The International Journal of Robotics Research, 1986, 5(1): 90-98

[6] Zhong M, Shen K, Seiferas J. The convergence-guaranteed random walk and its applications in peer-to-peer networks [J]. IEEE Transactions on Computers, 2008, 57(5): 619-633