基于混沌理论的网络视频即付即看方案*)

张 红[1] 李 波[1] 肖 迪[2] 廖晓峰[2]

(重庆工学院计算机学院 重庆400050)[1] (重庆大学计算机学院 重庆400044)[2]

摘 要 在对现有各种网络视频即付即看方案模型和混沌理论进行深入研究的基础上,利用混沌系统迭代过程的单向性构造出 Hash 支付链,实现了支付字据流和视频流的逐单位交换,保证了整个交换过程的完全公平性。方案结构简单,具有较高的安全性、较低的通信量和较快的执行效率。

关键词 网络视频,即付即看,混沌理论,Hash 函数链

A Chaos-Based Pay-Per-View Scheme for Network-Based Video Service

ZHANG Hong[1] LI Bo[1] XIAO Di[2] LIAO Xiao-Feng[2]

(College of Computer, Chongqing Institute of Technology, Chongqing 400050)[1]

(College of Computer, Chongqing University, Chongqing 400044)[2]

Abstract Based on the in-depth research on the existing Pay-Per-View models for network-based video service and chaos theory, the one-way property of chaotic iteration is utilized to construct Hash Function Chains, realize unit-by-unit release of the pay chain and video stream, and guarantee the fairness of the exchanging process. The scheme has simple structure, higher security, less traffic and greater processing efficiency.

Keywords Network-based video service, Pay-per-view, Chaos; Hash function chains

1 引言

随着宽带网络技术的高速发展,有偿网络视频服务越来越受到人们的欢迎,它可以保证用户在任何时间通过付出一定的费用而点播其感兴趣的节目,实现即付即看(Pay-Per-View, PPV)。但是,如何以较低的代价,安全高效地实现整个 PPV 过程的公平性,却是一个比较困难的问题。目前,此类问题已引起了学术界的广泛关注,文[1~3]提出了一些方案模型,但它们都完全局限于从传统密码学的角度出发,方案整体上并不太完善。

混沌密码技术是现代密码学发展的一个重要成果,具有很大的发展潜力,已经成为当前信息安全领域的一个研究热点。本文在对混沌密码技术进行了深入研究的基础上,设计了一个基于混沌理论的网络视频即付即看方案。该方案利用混沌系统迭代过程的单向性构造出 Hash 支付链,实现了支付字据流和视频流的逐单位交换,保证了整个交换过程的完全公平性:当服务商发现某个支付字据无效时可立即中断后续服务;当客户对服务不满意时也可主动请求停止服务;当网络发生中断,客户在中断恢复以后可请求继续服务。

2 基于混沌理论的网络视频即付即看方案

2.1 Hash 链技术的基本思想[1]

本文的公平支付方案利用了 Hash 链技术,该技术的基本思想是:用户随机地选择一个种子 m,分别计算其 Hash 值 $h(m), h^2(m), \cdots, h^n(m)$,其中 $h^n(m)$ 叫 Hash 链的根,设用户的私钥是 skc,用户对这个根签名 $\{h^n(m)\}skc$,然后发给远程服务器:$h^n(m)$ 和 $\{h^n(m)\}skc$。以后用户通过依次向服务器出示 $h^{n-1}(m), \cdots, h(m), m$,可以证明自己 n 次。这主要是利用了单向 Hash 函数的单向性,即:从 $h^i(m)$ 计算 $h^{i+1}(m)$ 容易,但从 $h^{i+1}(m)$ 计算 $h^i(m)$ 则非常困难。

2.2 利用混沌动力系统构造 Hash 函数链

混沌是在非线性动力系统中出现的一种确定性的、貌似无规则的伪随机过程,是普遍存在的复杂运动形式和自然现象。混沌系统对初始状态极度敏感;混沌系统具有自相似性,使得局部选取的混沌形态和整体完全相似;混沌系统的动力学行为极其复杂,不符合概率统计学原理,难以重构和预测;此外,混沌系统的迭代过程还具有单向性,混沌系统每次迭代都会产生完全不同的结果,而同一个混沌系统若系数和初值相同,将肯定产生完全相同的两个迭代序列。因此,可以利用混沌动力系统来构造 Hash 函数链[4,5]。

本文选择的混沌映射是 Logistic 方程:$X_{n+1}=bX_n(1-X_n)$,其中 $X_n\in[0,1]$,取定 $b=3.99999$。不失一般性,也可选用其它的混沌映射和相应的参数。经计算机仿真我们发现,当 $X_n\in[0.15,0.8]$ 时,迭代出的值分布比较均匀,因此我们可以在此区间中确定一个初值 X_0,再通过迭代即可生成 Hash 链:$X_0, X_1, X_2, X_3, X_4, X_5, \cdots, X_n$。

在实现的过程中,应该注意两点:

(1)从安全性的角度考虑,为了保证混沌方程的迭代值分布尽量均匀,我们在算法中设定所有的迭代值都必须在区间[0.15,0.8]中,因此,当迭代过程中得到该区间以外的值时应舍去,方程继续迭代直到产生该区间内的值才算一次成功的迭代。

(2)由于混沌系统对初始状态极度敏感,不同的计算机系统在计算精度上的微小差异可能会因为"蝴蝶效应"而造成误

*)本文受国家自然科学基金(No:60271019)、教育部重点科技项目基金(No:03115)和重庆市科委应用基础研究项目基金(No:7370)资助。张红 讲师,硕士生,主要研究方向:计算机信息安全,电子商务、电子政务等。

判。在算法中，我们事先约定对每次的迭代结果取某一个合适的有效位数，从而避免了此类问题的发生。

2.3 基于混沌理论的网络视频即付即看方案

本方案涉及到客户、服务商和经纪人，他们都已经知道使用的是什么混沌方程(即散列算法)。下面以客户准备向视频服务商购买某种视频服务为背景对方案进行说明。

视频服务商在网上公布视频节目目录供客户挑选，列出每个节目的简单介绍、收费单位 L(如1分钟、5分钟等)、需要的收费单位数 N 和价格 P 等。

客户在经纪人处建立一个帐户，并注入资金，由经纪人发给他一个支付字据证书，该证书要定期更新(如一个月或若干天等)，由此可以使那些有不良信用记录的人无法取得新的证书。

客户获得了支付字据证书，就表示从经纪人处获得了授权，可以制造自己的支付字据链。一个支付字据链代表了客户对于某个服务商的信用，它是一个 Hash 值的序列，链中的每个支付字据都具有相同的币值。客户生成一个新的支付字据链的步骤是：

(1)客户浏览视频服务商的视频节目目录，确定其准备购买的视频服务所需的收费单位数 N；

(2) 客户将在[0.15,0.8]中选定一个随机数 X_0作为自己的支付字据链的初值；

(3)代入 Logistic 方程对 X_0取 N 次 Hash 值；

(4)最终的支付字据链是$\{X_0, X_1, X_2, X_3, X_4, X_5, \cdots, X_n\}$，其中 X_n 是该 Hash 链的终值(根)。

支付方案的简单过程如图1所示：

(1)在第一次交换时，客户对自己的支付字据证书和支付字据链的终值(根)X_n 签名，作为对该链的承保书，并把承保书、第1个支付对$(X_{n-1},1)$和 X_n 发送给服务商；服务商验证 $h(X_{n-1})=X_n$ 是否成立，若成立就将第一个单位的视频流提供给客户，若不成立则马上终止服务。

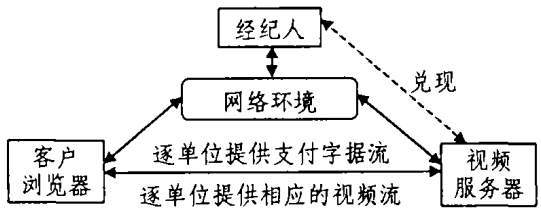

图1 网络视频即付即看方案模型

(2)从第二次交换开始一直到第 N 次交换，客户把第 i 个支付对(X_{n-i},i)传给服务商。服务商可以验证 $h(X_{n-i})=X_{n-i+1}$是否成立，当客户试图提供无效的支付字据链时，服务商可立即发现并中断后续服务；当客户对服务不满意时，就不再提供下一次的支付对，从而停止请求服务；当网络发生中断，客户在中断恢复以后可方便地请求继续服务。

(3)当交易结束时，经纪人负责从服务商处赎回所支付的支付字据链，从用户的帐户上划拨出已经花费掉的资金数额给服务商；同时把那些在交易过程中有不良信用记录的人记入被撤消支付字据证书的黑名单。

3 性能分析

与文[2]所提出的在线第三方协议模型的典型方案相比，本文采用离线第三方模式，只有在支付结束时才需要经纪人的介入，这样可以极大地减少系统的通信量，在第三方处不会形成瓶颈；此外，第三方并不接触交易双方的视频信息流本身，所以更为安全。

另外，由于本方案中主要涉及的是 Hash 函数计算，避免了以往种种公平交易方案中使用的众多的加解密计算；而且本方案充分利用了混沌动力系统的单向性来构造 Hash 函数链，大大简化了各种传统 Hash 算法的结构，所以在保证安全的前提下，和现有的类似方案相比，能极大地提高了整个方案的执行效率，降低了支付成本。

综上所述，本文提出的基于混沌理论的网络视频即付即看方案具有较高的安全性、较低的通信量和较快的执行效率，更为符合电子商务环境中的实际需要。

结论 宽带网络技术的高速发展，迫切需要对网络视频即付即看问题进行深入的研究。本文在对现有各种网络视频即付即看方案模型进行深入研究的基础上，基于混沌理论设计了一个的新的网络视频即付即看方案。该方案利用混沌系统迭代过程的单向性构造出 Hash 支付链，实现了视频流服务的逐单位释放，保证了整个交易过程的完全公平性。

本文提出的网络视频即付即看方案结构简单，具有较好的开放性，面对实际电子商务活动所不断提出的新需求，还可以考虑在现有协议的基础上进行改进，也可以和其它技术进行结合，比如保护数字视音频产品的数字水印技术等，这些都是我们未来将要进一步研究的方向。

参 考 文 献

1 Cunningham D, O' Mahony D. Secure Pay-Per-View Testbed [A]. In: Proc. of 1995 IEEE Intl. Conf. on Multimedia Computing and Systems. USA: IEEE Computer Society Press, 1995. 141～151

2 Franklin M K, Reiter M K. Fair exchange with a semi-trusted third party[C]. In: Proc. of the 4th ACM Conf. on Computer and Communication Security. New York: ACM Press, 1997. 1～5

3 姬东耀，王育民. 公平有效的 WEB 视频服务即付即看协议设计与分析. 西安电子科技大学学报，2001,28(4):425～429

4 李红达，冯登国. 复合离散混沌动力系统与 Hash 函数[J]. 计算机学报，2003,26(4):460～464

5 Caponetto R, Di Bernardo G, Di Cola E. A new chaotic system for the authentication and electronic certification procedures [DB/OL]. 0-7803-5682-9 IEEE, 1999. 1235～1238

6 陈谊，白少华，翁贻方. 基于混沌理论的文件安全系统[J]，计算机工程，2003,29(14):129～132