基于用户概率分组模型的密钥分发方法研究

屈 劲[1],葛建华[1],蒋 铭[2]
(1. 西安电子科技大学计算机网络与信息安全教育部重点实验室,陕西西安 710071;
2. 上海交通大学电子信息学院,上海 200030)

摘 要: 条件接收系统是付费电视系统的重要组成部分,而其中密钥分发的效率和安全性又是影响条件接收系统性能的关键因素. 本文基于用户概率模型提出了用户霍夫曼树分组模型及相应密钥分发方法,该方法具有最优的分发效率.

关键词: 条件接收; 付费电视; 密钥分发; 霍夫曼树
中图分类号: TN949 **文献标识码**: A **文章编号**: 0372-2112 (2003) 08-1266-03

On Key Distribution Based on Grouping User with Probability

QU Jin[1], GE Jian-hua[1], JIANG Ming[2]
(1. *Key Lab of Computer Network and Information Security, Xidian University, Ministry of Education, Xi'an, Shaanxi* 710071, *China*;
2. *School of Electronics & Information Technology, Shanghai Jiaotong University, Shanghai* 200030, *China*)

Abstract: Conditional access system is the crucial part of Pay-TV System, and the efficiency and security of key distribution are the main factors which influence the performance of conditional access system. In this paper we proposed a new key distribution scheme on the basis of grouping users with their probability, and prove that this scheme has optimal distribution efficiency.

Key words: conditional access; pay-TV; key distribution; Huffman tree

1 引言

随着数字电视、多媒体和宽带网技术的迅猛发展,如何保护投资者和产品开发者的利益已经成为保障信息产业顺利发展的重大问题. 除了需要完善相应法律体系[1],更需要发展相应技术,条件接收 CA(Conditional Access)就是在这种背景下发展起来的. CA 系统主要用于付费电视业务,保证只有付费用户或预定某项业务的用户可以收看某个节目或使用某项业务,而其他用户不能收看该节目或使用该项业务,这都是通过给用户分发数据加密密钥来实现的. 目前国外已经有一些系统投入使用,如 EUROCRYPT[2]、DSS、Vidocrypt、Sumulcrypt、CryptoWorks 等.

CA 系统同其他安全系统相比较具有下述特点:被保护的信息传输速率高、信息价值低;同时考虑到用户对用户端解码器成本的经济承受能力,条件接收系统要求在保证一定安全的条件下,尽量降低接收端的复杂度.

安全、有效的密钥分发是 CA 系统安全、降低通信成本和用户接收解码器复杂度的关键. 目前 CA 系统中常用的密钥分发方式有两类:一类基于公钥密码体制,如 RSA;另一类基于对称密码体制,如密钥层次结构分发[3,4,5].

层次结构分发是一种有效的密钥分发方法,在保证安全性的前提下提高了密钥分发效率. 本文在密钥层次结构分发的基础上根据用户离开业务组的概率特性,提出了一种新的层次密钥分发方法,用户 Huffman 树分组密钥分发方法,并证明该方法的密钥分发效率高于非概率层次结构密钥分发方法,具有最优的分发效率.

2 用户概率分组模型

经过一段时间,用户可能继续购买某个电视业务,也可能转而购买新的电视业务,为保证用户能收视新的业务,而不能收视不再购买的业务,必须给用户定期更新密钥,因此用户离开概率将影响 CA 系统的密钥分发效率,这也就是采用概率模型分析 CA 系统密钥更新的主要原因.

本文主要研究两种依据概率分组的密钥分发问题,平衡树分组和 Huffman 树分组:平衡树实际是一种非概率分组方法,具有构造、维护简单,密钥更新量较小的特点;Huffman 树的分组可以充分利用将离开概率小的用户可以安排在路径长的树枝上,而概率大的用户安排在路径短的树枝上以减少平均密钥分发量.

2.1 密钥树及更新

传统的层次密钥分发是这样构成的,首先将若干用户分成一个小组,每个小组分配一个组密钥,这些小组再合成更大

收稿日期:2001-11-19;修回日期:2002-06-04
基金项目:国家教育部高校骨干教师资助项目;陕西省自然科学基金(No. 2002f08)

的组,直到所有用户都共享一个组密钥 SK(Session Key),在 CA 系统中 SK 用于加密传输加扰控制字 CW(Control Word),CW 用于电视节目加密.这种层次结构类似于一个方向树,因此又被称为密钥树.

密钥树中每一个节点都代表一个密钥,根节点是所有用户共享的组密钥,叶节点是用户的私人密钥,同时也是用户的身份标志.为了便于描述密钥树结构作如下定义:树叶到树根的方向称为树的方向;对某节点而言,连接该节点指向根节点的路径称为接出路径,连接叶节点指向该节点的路径称为接入路径;树的高度(层数) h 定义为树上最长的单向路径;树的维数 d 定义为树中节点的最大接入路径数.

为保证系统安全,当用户加入或离开该组时,必须更新密钥树,保证新用户可以利用该业务,离开用户不能再使用该业务.

2.2　用户概率分组模型

设某业务组的合法用户全体为 $U=\{u_1,u_2,\cdots u_n\}$,用户 u_i 离开组的概率为 p_i,对于 $1\le i\le n$,满足 $\sum_{i=1}^{i=n}p_i=1$,根据信息论[6]易知:如果选取 $h_i=\lceil\log_d p_i\rceil$($\lceil x\rceil$表示大于或等于 x 的最小整数),则用户在密钥树中平均高度的下限为:

$$\bar{h}\ge-\sum p_i\log_d p_i \tag{1}$$

因此一个用户离开的密钥更新量理论下限为:

$$\bar{s}=d\bar{h}-1\ge-d\sum_{i=1}^{n}p_i\log_d p_i-1 \tag{2}$$

2.2.1　平衡树

平衡树[5]构造简单,得到了深入研究.因为仅满树存在解,所以本文只研究满树情况.设叶片数为 m,平衡树为满树应满足下述条件:

$$m=d^h \tag{3}$$

构造平衡树,首先计算总叶片数 m,给定 h 或 d,根据式(3)判断用户数 n 是否满足满树条件,若满足则 $m=n$;若不满足,根据给定 d 求树高 h:

$$h=\lceil\log_d n\rceil \tag{4}$$

然后依次每 d 个用户合成一组(高一级节点),每 d 组合成一个更大的组(更高一级节点),直到树根.由上述过程可知平衡树的构造与用户离开概率无关.

2.2.2　Huffman 树

Huffman 码是信源编码中平均码长最短的非等长码,本文将利用它来构造最佳的密钥分层结构.构造 d 维 Huffman 满树时,密钥树从根开始分裂可形成 d 个叶节点,叶节点每次再分裂可增加 $d-1$ 个叶节点,因此如果分裂 s 次,则 Huffman 满树的总叶片数 m 应满足下式:

$$m=(s-1)(d-1)+d \tag{5}$$

构造 Huffman 树,给定 h 或 d,首先计算总叶片数 m,验证用户数 n 是否满足式(5),若满足,$m=n$;若不满足,则:

$$m=\left\lceil\frac{n-d}{d-1}\right\rceil(d-1)+d \tag{6}$$

为保证满树需增加 $m-n$ 个概率为 0 的空用户位置,可以证明 $m-n<d-1$.

根据用户离开概率对用户分组.先将 m 个用户按概率大小排队,概率大的排在上面,概率小的排在下面;取用户删除概率最小的 d 个用户分成一组形成组节点,并将这些用户的概率相加作为该节点的概率,再将该组节点和其他用户重新排队,再取概率最小的 d 个节点或用户组成一个组节点,如此下去直到树根构成一个 Huffman 满树,树根的概率为 1,最后给节点安排密钥,这就构成了密钥 Huffman 分层结构.为保证满树,加入的删除概率为 0 的空用户虽分配密钥,但实际是冗余用户,这样分配密钥仍具有最小平均高度.

3　基于用户概率分组模型的密钥分发方法性能分析

在保证安全性前提下,衡量一个密钥分配方法性能的主要指标是单位时间内的密钥分发量.而 CA 系统的密钥分发量主要取决于一个用户离开时所需的密钥更新量,本文主要通过分析一个用户离开时的密钥更新量来研究用户概率分组模型的密钥分发方法的性能.

3.1　平衡树模型

在平衡树模型中,任意用户离开时的密钥更新量为:

$$s_i=dh-1 \tag{7}$$

因此一个用户离开时平均密钥更新量:

$$\bar{S}=\sum_{i=1}^{n}p_i s_i=dh-1 \tag{8}$$

由式(8)可以看出,采用概率平衡树分组模型和非概率平衡树模型分组模型的性能一样.

3.2　Huffman 模型

在 Huffman 树中一个用户离开引起的密钥更新量和用户位于的层数有关,为了方便描述用户离开和密钥更新量的关系,定义用户 u_i 位于 L_i 层,s_{i,L_i} 表示 L_i 层的 u_i 离开的密钥更新量

$$s_{i,L}=L_i d-1 \tag{9}$$

一个用户离开时的平均密钥更新量

$$\bar{S}=\sum_{i=1}^{n}p_{i,l}s_{i,L}=d\sum_{i=1}^{n}p_{i,l}L_i-1 \tag{10}$$

3.3　性能比较

结合式(8)、(10)可知,如果 d 相同,则 Huffman 模型优于平衡树模型的条件是:

$$\sum_{i=1}^{n}p_{i,l}L_i<h \tag{11}$$

而概率模型中,用户离开概率等概时熵最大,所以

$$\sum_{i=1}^{n}p_{i,l}L_i<\sum_{i=1}^{n}\frac{1}{n}\left\lceil-\log_d\frac{1}{n}\right\rceil=\lceil\log_d n\rceil \tag{12}$$

而根据式(4)可知式(11)显然成立.

显然 $L_i\ge-\log_d p_i$,因此式(2)是一个用户离开时的密钥更新量下限,Huffman 树为最优的分层密钥分发方案,优于平衡树方案.

4　结束语

密钥管理系统是 CA 系统的核心,其密钥分发效率和安

全性直接影响系统的传输负荷和安全性,本文提出基于用户离开概率的 Huffman 分层模型的密钥分发方法,证明该方法具有最优的密钥分发性能,同时还给出了 CA 系统的密钥分发量下限,对 CA 系统的密钥管理具有一定指导意义.

参考文献:

[1] The European Commission Green Paper. Legal protection for encrypted services in the internal market [Z]. 1996.

[2] V Lenoir. EUROCRYPT, a successful conditional access system [J]. IEEE Trans Consumer Electronics, Aug. 1991, 37(3): 432 - 436.

[3] E Cruselles, J Luís, M Soriano. An overview of security in eurocrypt conditional access system [A]. Proc. IEEE GLOBECOM'93 [C]. Houston, 1993: 188 - 193.

[4] F K Tu, C S Laih, H H Tung. On key distribution management for conditional access system on pay-TV system [J]. IEEE Trans. Consumer Electronics, Feb. 1999, 45(1): 151 - 158.

[5] C K Wong, M G Gouda, S S Lam. Secure group communications using key graphs [A]. Proceedings of ACM SIGCOMM'98 [C]. New York: ACM Press, 1998. 68 - 79.

[6] 周炯磐, 丁小明. 信源编码理论(M). 北京: 人民邮电出版社, 1996: 9 - 27.

作者简介:

屈 劲 男, 1971 年生于陕西宁强县, 1994 年毕业于重庆大学应用物理系, 获学士学位, 1999 年于西安电子科技大学获硕士学位, 目前为西安电子科技大学在读博士生, 主要兴趣方向是信息安全和数字电视.

葛建华 男, 1961 年 9 月生于江苏省南通市, 现西安电子科技大学教授, 博士生导师, 主要兴趣方向为数字电视、信号处理、密码学.