一种高效的LKH方案研究

康晓辉,马占梅
(西安电子科技大学 计算机学院,陕西 西安 710071)

摘 要:提出了一种新的逻辑密钥树(LKH)改进方案,每个用户可以根据自己的私钥通过计算得到加密密钥,任何成员的变化都不需要更新其它用户的密钥,从而减少了更新密钥时的额外开销,组管理器存储的密钥数,叶子节点存储的密钥数和用户离开/加入时的加解密数。研究了密钥的周期更新,有效地防止多个非法用户共谋,提高了组播的安全性能。

关键词:组播;RSA;逻辑密钥树;周期更新
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2009)02-0176-03

One High Efficient Scheme Based LKH

KANG Xiao-hui, MA Zhan-mei
(School of Computer Science, Xidian University, Xi'an 710071, China)

Abstract: In this paper, it advanced one new LKH method that every user could calculate encrypted key by oneself private key. When anyone changed, the others needn't change their private key. Therefore this method could reduce the cost of updating key, the storage key of group controller, the storage key of leaf, the encryption and decryption time when one user leave or join in. In addition, discussed the period updating, which can prevent some lawless users conspire together, and advance the capability of multicast.

Key words: multicast; RSA; logical key hierarchy; period updating

0 引 言

随着英特网、数字电视、数据广播的迅猛发展,在过去的点到点通信模式的基础上出现了组通信模式。这种通信模式的主要特点是通信不再被限制于两点之间,而是一点同时和多点通信或多点之间通信。组播在虚拟会议,以及网络游戏、多媒体实时点播上都有广泛的应用,所以越来越被更多的人所重视。大多数组播通信的安全都依赖于组播密钥,随着群用户数的大幅增长,使得组播密钥存储量大,加解密次数多的问题越来越凸显,所以国内外很多专家学者从如何显著减少组播密钥存储量及加解密次数提出了众多算法,其中逻辑密钥树(LKH)[1~7]这类方案因具有良好的前/后向保密性,较少的加解密次数及相对小的密钥存储量而成为主流的管理方案。文献[6]对LKH方案进行了改进,当组播组用户巨大时,其开销仍然很大,还是不能满足日益增长的组播需求。文献[8]提出了基于RSA的组播管理方案,该方案存在一定的缺陷,当多个用户同时离开多播组时,组管理器的计算开销过大,另外方案没有采用分层技术,所有的用户都由组管理器直接管理,如果组管理器受到攻击或者其它故障而失效,将使得整个多播组崩溃,后果是比较严重的。为了进一步提高LKH的性能,文中对LKH算法进行了改进,使得组播密钥的存储量从 $O(\log_d N)$ 减少到 $O(1)$,不需要 $O(2\log_d N)$ 次加解密。本方案还从防止同谋和保证用户密钥的新鲜性(保证用户私钥在周期时间内得到更新)进行了研究,使得组播有更好的安全性。性能分析证明了本方案的优点和可行性,本方案具有较强的实用性。

把密钥管理面临的主要问题归结如下:

(1) 前向加密:确保组成员在退出组后,除非重新加入,否则无法再参与组播,包括获知组播报文的内容和发送加密报文。

(2) 后向加密:确保新加入的组成员无法破解它加入前的组播报文。

(3) 同谋破解:避免多个组员联合起来破解系统(或减少发生的概率)。

(4) 密钥生成计算量:通常,协同的密钥生成需要较大的计算量,当节点的计算资源不充足或密钥更新频繁时,要考虑密钥生成给节点带来的负载。

收稿日期:2008-05-23
作者简介:康晓辉(1983-),男,陕西宝鸡人,硕士研究生,主要研究方向为组播密钥的管理及其分发;导师:杨世勇,副教授,硕士生导师,主要研究方向为网络信息安全、多媒体通信、密码学及信息隐藏、数字水印。

1　LKH 算法的描述

在 LKH 机制中,有一个组管理器 GC,用以对组内成员进行管理[1,2,7],逻辑密钥树采用 d 叉树结构来管理,每个叶子节点都对应一个物理实体(用户),还有为减少加解密开销而虚拟的中间节点,其并不代表任何实际意义。图 1 是一个逻辑密钥树的示意图(为了论述方便,以一棵平衡二叉树为例来进行讨论,逻辑密钥树对此并不要求)。组成员 U4 对应的叶子节点是 k44,U4 知道自己到 GC 路径上所有节点的密钥(k44,k32,k21,k11)。逻辑密钥树的层次结构还使得中间节点对应的密钥可以被用来为小组的通信加密。比如,U1,U2,U3,U4 可以利用 k21 来进行组内更小范围的安全通信[7]。

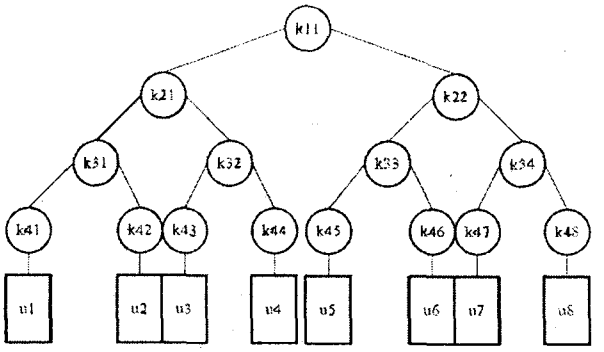

图 1　逻辑密钥树(LKH)

当用户 U3 离开时,从下到上依次更新其路径上的密钥(k32,k21,k11)为(k32′,k21′,k11′),然后多播$\{\{k11'\}_{k21'},\{k11'\}_{k22},\{k21'\}_{k31},\{k21'\}_{k32'},\{k32'\}_{k44}\}$,$kij$ 表示原来的密钥,kij'表示更新后的密钥,i 表示该节点的层数,j 表示该节点在 i 层的编号,$\{A\}_B$ 表示用 B 加密 A。可以看出对于有 N 个用户的 d 叉树而言,GC 存储的密钥数为 $(d^{\lceil \log_d N\rceil+1}-1)/(d-1)$,删除/加入一个用户需要加解密的次数为 $2\lceil \log_d N\rceil$,叶子结点存储的总密钥数为 $N(\lceil \log_d N\rceil+1)$。

对于大型多播组而言,LKH 方案的各项开销是比较大的,所以希望提出新的方案以减少各项开销。

2　改进后的 LKH 算法

2.1　算法的提出

随机选取两个足够大的素数 p,q[8],计算:

$$\mathrm{PubInf}_1 = pq \tag{1}$$

和 PubInf_1 的欧拉函数

$$\varphi(\mathrm{PubInf}_1) = (p-1)*(q-1) \tag{2}$$

其中 $p,q,\varphi(\mathrm{PubInf}_1)$是保密的,$\mathrm{PubInf}_1$ 是公开的,合法用户 Ui 拥有私钥 ki,ki 是一个大素数,且用户之间的私钥是互不相关的,对于当前多播组成员(U1,U2,…,Un),所对应的私钥为(k1,k2,…,kn),计算:

$$\mathrm{GCK} = k_{11} = k_1 * k_2 * \cdots * k_n \tag{3}$$

其中 GCK 是组管理器 GC 的密钥,也可称之为加密密钥,$\forall Ui$,

$$\mathrm{PubInf}_2 = \mathrm{GCK}/\mathrm{PubInf}_1 \tag{4}$$

$$\mathrm{PrivateInf} = \mathrm{GCK} \bmod \mathrm{PubInf}_1 \tag{5}$$

其中 PubInf_2 是公开的,PrivateInf 是不公开的。

$$\mathrm{GCK} = \mathrm{PubInf}_2 * \mathrm{PubInf}_1 + \mathrm{PrivateInf} \tag{6}$$

$\forall Ui$,有

$$\begin{aligned}&\mathrm{PubInf}_2 * \mathrm{PubInf}_1 \bmod ki\\ &=(\mathrm{GCK}-\mathrm{PrivateInf})\bmod ki\\ &=(\mathrm{GCK}\bmod ki-\mathrm{PrivateInf}\bmod ki)\bmod ki\\ &=(k1*k2*\cdots*kn \bmod ki-\mathrm{PrivateInf}\bmod ki)\\ &\quad \bmod ki\\ &=(ki \bmod ki-\mathrm{PrivateInf}\bmod ki)\bmod ki\\ &=(ki-\mathrm{PrivateInf})\bmod ki\\ &=ki-\mathrm{PrivateInf}\end{aligned} \tag{7}$$

由式(7)可以得到

$$\mathrm{PrivateInf} = \mathrm{PubInf}_2 * \mathrm{PubInf}_1 \bmod ki - ki \tag{8}$$

$$\mathrm{GCK} = \mathrm{PubInf}_2 * \mathrm{PubInf}_1 + \mathrm{PrivateInf} \tag{9}$$

用户 $Ui(i=1,\cdots,n)$可以利用自己的私钥 ki 和公开信息($\mathrm{PubInf}_1,\mathrm{PubInf}_2$)通过式(8)计算得到 PrivateInf,然后再根据式(9)得到组管理器密钥 GCK。

2.2　加入操作

当成员向组控制器申请加入多播组时,组控制器首先验证成员的身份,确认后把该用户插入逻辑密钥树中最优位置[4],为该成员节点产生随机大素数 kij(i 表示层数,j 表示在该层的序号)作为其私有密钥,并通过安全通道分发给该成员。如新加入的成员为 U4,GC 产生大素数 k44,并通过安全通道发送给成员 U4,为了保证后向的安全性,必须更新加入用户 U4 路径上所有节点的密钥[7](k32,k21,k11)为(k32′,k21′,k11′),其中 k32′=k43 * k44,k21′=k31 * k32′,k11′ * k22,GCK′=k11′组管理器 GC 根据(4)式计算得到($\mathrm{PubInf}_1,\mathrm{PubInf}'_2$)并把公开信息($\mathrm{PubInf}_1,\mathrm{PubInf}'_2$)以多播的方式发送给当前的所有组成员。在接下来的多播通信中用 GCK′对多播内容进行加密或者加扰[7],新加入的用户 U4 和原来的用户(U1,U2,U3,U5,U6,U7,U8)都可以用自己的私钥(k41,k42,k43,k44,k45,k46,k47,k48)和公开信息($\mathrm{PubInf}_1,\mathrm{PubInf}'_2$)根据式(6)计算得到更新后的 GCK′。而对于新加入的用户而言,由于其拥有的私钥 k44 并未参加前面 GCK 的生成,所以 U4 无法得到 GCK,从而达到后向保密性。

2.3　离开操作

当成员离开某个特定多播组时,为了保证前向安

全性，组管理器必须更新其路径上所有节点的密钥，假如离开的用户为 U4，首先吊销它的密钥 k44[9]，并更新其路径上的密钥组(k32，k21，k11)为(k32′，k21′，k11′)，其中 k32′ = k43，k21′ = k31 * k32′，k11′ = k21′ * k22，GCK′ = k11′，组管理器 GC 根据式(4)计算得到 $(PubInf_1, PubInf'_2)$，并把公开信息 $(PubInf_1, PubInf'_2)$ 以多播的方式发送给当前的所有组成员。剩余用户(U1，U2，U3，U5，U6，U7，U8)用自己的私钥(k41，k42，k43，k45，k46，k47，k48))和公开信息 $(PubInf'_1, PubInf'_2)$ 据式(6)计算 GCK′，如图 2 所示，kij′表示更新后的密钥。由于离开节点的私钥不再参与 GCK′的生成，即离开用户无法解密离开之后的加密信息，从而达到前向保密性。

2.4 密钥的周期更新

在大量用户离开多播组时，为了防止他们共谋，同时保证私钥的新鲜性，必须对密钥进行批量或者周期更新，更新算法如下：GC 在大量用户加入/离开多播组后，或者在特定的时间段 ΔT 之后，GC 产生一个新密钥 K 作为节点($\lceil \log_2 N \rceil + 1$，rad mod N)的新密钥，这里的 rad 是一个随机数，N 是当前用户的节点数，如果编号为 rad mod N 的节点不存在，那就重新产生随机数，直到存在为止。并且以 $f(T, \Delta T) \bmod N$ 为步长依次从节点 rad mod N 开始旋转其它节点的密钥，这里的 N 是当前用户节点数，f 是单向函数(如 MD5 算法)，T 是当前时间。

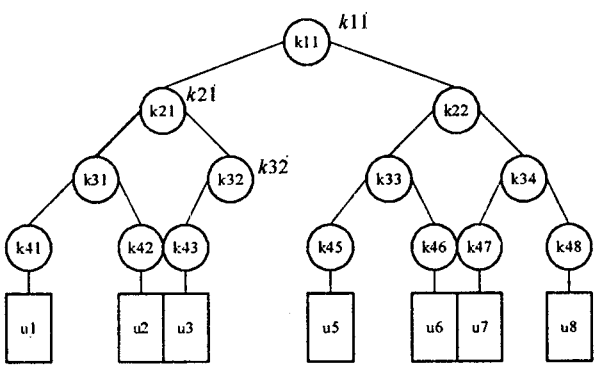

图 2 改进后的 LKH 用户离开示意图

以图 1 为例，假如用户 U2，U3，U5，U7 离开，可以把节点分为离开用户节点组 Leave(U2，U3，U5，U7)和当前用户节点组 Left(U1，U4，U6，U8)，并且假设 rad mod $N = 6$，$f(T) \bmod N = 2$，GC 为 U6 产生新的密钥 k46′，经过更新之后的当前用户节点组 Left(U1，U4，U6，U8)拥有的更新后的私钥组(k41′，k44′，k46′，k48′)为(k46，k48，k46′，k41)。下面来证明离开的用户组 Leave(U2，U3，U5，U7)无法用自己拥有的私钥(k42，k43，k45，k47)组共谋得到 GC′。

更新之前：

$K_{Left} = k41 * k44 * k46 * k48$，$K_{Leave} = k42 * k43 * k45 * k47 *$，$GC = K_{Left} * K_{Leave}$

更新之后：

$GC' = K_{Left}' = k41' * k44' * k46' * k48' = k46 * k48 * k46' * k41$，可以看出 $K_{left} * K_{Leave} \neq GC$，所以 Leave(U2，U3，U5，U7)无法用自己拥有的私钥组(k42，k43，k45，k47)解出或者得到 GC′的相关信息，从而提高了多播组的安全性，如图 3 所示。另外这样也可以用只产生一个新密钥的代价来实时的更新所有用户的密钥。

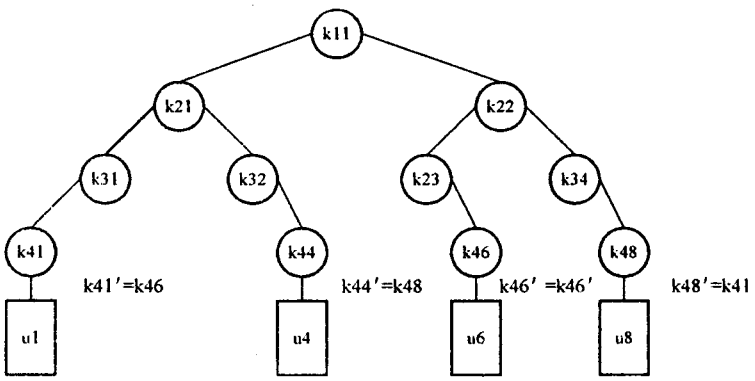

图 3 改进后的 LKH 周期更新示意图

2.5 算法性能分析

从表 1 可以看出，改进后的算法在 GC 存储的密钥数，叶子节点存储的密钥数，用户离开/加入时的加解密数方面都有很大的改进，具有良好的扩展性。其在大型多播组中的应用前景是非常可观的。

表 1 LKH 改进方案和 LKH 方案的性能比较

	LKH	改进后的算法
GC 存储的密钥数	$(d^{\lceil \log_d N \rceil + 1} - 1)/(d-1)$	1
叶子节点存储的密钥数	$\lceil \log_d N \rceil + 1$	1
用户离开/加入时的加解密数	$2\lceil \log_d N \rceil$	0
用户离开/加入时的通信量	$\lceil \log_d N \rceil + 1$	$\lceil \log_d N \rceil + 1$
扩展性	良好	良好

3 结束语

随着互联网的广泛应用，组播得到极大的发展，其安全性尤其是密钥的动态更新是个值得关注的问题。文中在 LKH 的基础上结合 RSA 算法对原来的算法进行了改进，在性能上得到很大的提高，有效地防止了共谋，也保证了用户密钥的新鲜性，具有很好的安全性和扩展性，适合于大型多播组，有较大的应用价值。

参考文献：

[1] Kei Cheng，Gouda M，Lam S S. Secre Group Communications

(下转第 182 页)

```
end if
}}
end;
```

在算法的实现中，不是先生成所有的候选项目集再确定频繁项目集，而是生成一个候选项目集后就计算其频繁度，减少内存占用，提高算法的效率。

3.3 结果描述

数据挖掘将获取的信息以便于用户理解和观察的方式反映给用户，这时可以利用可视化工具。对于DM系统的挖掘结果，可以用自然语言、图形、表格等多种方式进行表示。在本系统中采用自然语言的方式表示。规则 A=>B 解释的形式为：加强对课程 A 的学习，有助于课程 B 的学习。其中前件 A 和后件 B 均可以包含任意多个属性。并且系统向用户推荐一个课程先后学习的序列。

由频繁项集 L_4 输出的一些关联规则：

加强对《计算机数学基础》《电子技术》《计算机组成原理》的学习，有助于课程《计算机体系结构》的学习。

加强对《计算机数学基础》《电子技术》的学习，有助于课程《计算机组成原理》《计算机体系结构》的学习。

加强对《计算机数学基础》的学习，有助于课程《电子技术》《计算机组成原理》《计算机体系结构》的学习。

课程推荐序列：《计算机数学基础》=>《电子技术》=>《计算机组成原理》=>《计算机体系结构》可由系统给出几种挖掘所得的规则形式及推荐课程设置的序列，给用户提供参考，由决策者决定所采用的规则及序列，做出相应的决策，指导学员选课，以帮助学员更好地完成各门课程的学习。

4 结束语

该系统实现了一个完整的数据挖掘过程，用户只要提供必要的数据，系统就可以自动地对选定的数据库进行分析，并且返回用户需要的信息，帮助用户做出决策，从而帮助学员选课及进一步学习，起到了很好的促进作用，具有一定的实用价值。同时数据挖掘技术已经在许多领域取得好的应用，随着数据的不断增长，把数据挖掘技术应用到远程教育教学中，能够较客观实时地反映问题，这一研究也对远程教育教学管理提出了很好的建议。

参考文献：

[1] Agrawal R, Imielinski T, Swami A. Mining Association Rules between Sets of Items in Large Database[C]//In SIGMOD' 93. Washington, DC: [s. n.], 1993: 207 - 216.

[2] Han Jiawei, Kamber M. 数据挖掘概念与技术[M]. 范 明，孟小峰等译. 北京：机械工业出版社，2003: 150 - 221.

[3] 朱 明. 数据挖掘[M]. 合肥：中国科学技术大学出版社，2002: 129 - 140.

[4] 程涛远. 基于园区网络的数据仓库相关技术的研究[D]. 济南：济南大学，2002: 36 - 40.

[5] 贾彩燕，倪现君. 关联规则挖掘研究述评[J]. 计算机科学，2003, 30(4): 145 - 148.

(上接第 175 页)

versity of Cambridge, 1996.

[13] 林 榕. 基于图像的信息隐藏技术综述[J]. 装备制造技术，2007(7): 91 - 93.

[14] 罗建禄. 图像数字水印技术综述[J]. 重庆工商大学学报：自然科学版，2007, 24(1): 10 - 11.

[15] Kutter M, Bhattacharjee S K, Ebrahimi T. Towards second generation watermarking schemes[C]// in Proc. IEEE Int. Conf. Images Processing: vol. 1. Kobe, Japan: [s. n.], 1999: 320 - 323.

[16] Moulin P, O'Sullivan J A. Information - Theoretic Analysis of Information Hiding[J]. IEEE Transaction on Information Theory, 2003, 49(3): 563 - 593.

(上接第 178 页)

Using Key Graphs[J]. IEEE/ACM Transaction on Networking, 2000(8): 16 - 30.

[2] Moyer M, Rao J, Rohatgi P. A survery of security issues in multicast communicastions[J]. IEEE Network, 1999, 13: 12 - 23.

[3] Wallner D, Harder E, Agee R. Key management for multicast: Issues and architecture[S]. IETF RFC 2627, 1999.

[4] Kwak D W, Lee Seung Joo, Kim Jong Won, et al. An Efficient, LKH Tree, Balancing Algorithm for Group Key Management[J]. IEEE Communication, 2006, 10(3): 222 - 224.

[5] Son Ju - Hyung, Lee Jun - Sik, Seo Seung - Woo. Energy Efficient Group Key Management Scheme for Wireless Sensor Networks[M]//IEEE, Invited Paper. [s. l.]: [s. n.], 2007.

[6] 康巧燕，孟相如，王建峰，等. 基于逻辑层次树的动态组播密钥管理改进方案[J]. 计算机工程，2007(8): 123 - 125.

[7] 徐明伟，董晓虎，徐 恪. 组播密钥管理的研究进展[J]. 软件学报，2004, 15(1): 141 - 149.

[8] 周 杰，张金焕，王全迪，基于 RSA 的组播加密方法及其密钥管理方案[J]. 大连理工学报，2005, 45(10): 122 - 125.

[9] 李新国. 数字内容保护系统中的认证和密钥管理技术研究[D]. 西安：西安电子科技大学，2006.