

批量密钥更新中密钥树的概率组织方法研究

赵克淳, 许 勇, 张 伟

(安徽师范大学 数学计算机科学学院, 安徽 芜湖 241000)

摘 要: 可缩放组密钥更新是大型动态组通信需要面对的一个重要问题。当前, 最有效的组管理技术是基于 LKH 机制的, 且 LKH 树通常被组织成平衡二叉树。在对批量密钥更新和成员行为进行分析的基础上, 结合星型结构和树型结构, 给出了一种密钥树的概率组织方法。该方法基于成员的变动概率将其分类, 每类关联一棵最优子树, 从而进一步减小了密钥更新开销, 较好地解决了多播组中异构成员变化带来的组密钥更新问题。实验结果表明, 密钥树的概率组织方法显著优于平衡二叉树, 且更具有一般意义。

关键词: 安全多播; 批量密钥更新; 密钥树; 概率组织

中图分类号: TP309

文献标识码: A

文章编号: 1673-629X(2007)12-0140-04

Study on Probabilistic Organization of Key Tree in Batch Group Rekeying

ZHAO Ke-chun, XU Yong, ZHANG Wei

(College of Mathematics and Computer Science, Anhui Normal University, Wuhu 241000, China)

Abstract: Scalable group rekeying is one of the biggest challenges that need to be addressed to support secure communications for large and dynamic groups. Currently, the most efficient techniques for multicast key management are based on the logical key hierarchy (LKH) scheme and LKH trees are always organized as balanced binary trees. Based on batch group rekeying and group member's behavior, propose a new method; probabilistic organization of the key tree, combining star structure and tree structure. The method classifies the members based on their changing probability and each class corresponds to an optimal tree, so it further decreases the rekeying overhead. The method can solve much better the problem of group rekeying with heterogeneous group members. Simulation results show that the method is more generalizing than others.

Key words: secure multicast; batch group rekeying; key tree; probabilistic organization

0 引言

多播作为一种非常有效和可缩放的组通信技术, 其应用(如视频点播、在线拍卖、远程电信会议等)需要一个安全的通信模型。多播安全通常采用组成员共享同一个组密钥的方式实现。为了实现多播的前向和后向安全性(即离开成员应不能解密其离开后的组通信内容和新加入成员应不能解密其加入前的组通信内容)^[1], 每次成员变化都要更新这个组密钥并分发给所有授权用户。星型结构和逻辑密钥树(logical key hierarchy, LKH)是常用的密钥管理方案^[2]。实际上, 星型结构又可看成树高为 1, 维数为成员总数的 LKH 的一

个特例。密钥更新是实现安全多播的关键。在一个大型多播通信中, 如果组成员变化非常频繁, 单个成员的实时密钥更新算法存在低效(inefficiency)和失序(out of sync)问题, 因此, 可采用批量密钥更新方法, 即周期性地对组密钥更新^[3]。批量密钥更新实际上是安全性和性能两方面的折衷, 在损失部分安全性的基础上提高了密钥更新效率, 减少了计算和通信开销。现有的批量密钥更新方法大多数基于 LKH, 但是由于 LKH 方法的提出基于实时密钥更新, 因此, 在批量密钥更新下, 其有效性和合理性需要重新予以考虑。

目前, 批量密钥更新方式通常使用一棵平衡密钥树, 并未考虑成员的行为特征, 因而其实际效率并不理想。为此, 文献[4]对于具有相同行为特征的成员(即成员加入、离开多播组的概率相同), 给出了一种批量密钥更新最优密钥树结构。这种特殊的树型结构在满足组成员具有相同的行为特征的前提下明显优于传统的平衡树。但是, 在实际多播应用中, 由于网络的异构

收稿日期: 2007-03-06

基金项目: 安徽省高校自然科学基金重点项目(2005KJ0092D)

作者简介: 赵克淳(1983-), 女, 安徽芜湖人, 硕士研究生, 研究方向为计算机网络、网络安全; 许 勇, 博士, 教授, 研究方向为计算机网络、网络安全。

特性以及多播内容的差异,参与同一多播组的成员可能会表现出多种不同的行为特征,因此,这种密钥树结构在实际应用中不能发挥其应有的作用。Selcuk 等指出考虑到成员的变动概率使用一个非平衡的密钥树更有效^[5]。在此基础上,文献[6]结合文献[7]中关于成员行为的研究结果,提出将密钥树分成了两部分:S-partition 和 L-partition。S-partition 用于存放参与多播时间较短的成员密钥;而 L-partition 用于存放参与多播时间较长的成员密钥。文献[8]对文献[6]进行了扩展,提出一种多级密钥树。但是上述这些文献中并没有明确密钥树的具体分割,给实际应用带来困难。通过对成员具有相同行为特征的多播组的密钥树的研究,笔者得出树的组织结构与成员变动概率之间的关系。文中将其结果引入多播组的密钥树的组织结构设计中,给出密钥树的一种概率组织方法,即依据成员变动概率对成员进行分类,进一步减小密钥更新开销。

1 密钥树的概率组织方法

1.1 成员具有相同变动概率的多播优化树

基于 LKH 的批量密钥更新,可以有效地减少密钥更新量,在整体上减少管理者的计算开销和网络通信开销,提高密钥更新可靠性。但是存在这样的事实:当多播组成员具有相同的变动概率时,如果将密钥树层以下的子树看成特殊的叶结点,那么,一次批量密钥更新中,这些特殊的子树均可能有成员发生变化,从而导致整棵密钥树 l 层以上(含 l 层)结点全部需要更新。对此,一种基于 LKH 的优化结构被提出,即将原先的密钥树设计成一种特殊的树型结构,其中,根结点对应的度数适当增加,其子树仍保持原有结构不变。文献[4]提供了一个批量密钥更新最优密钥树结构,即一棵根结点度数为 2^a ($a > 1$)、中间结点度数为 4、底层结点度数为 2 或 4 的平衡树。笔者通过理论证明和实验验证,得到 a 和成员变动概率 p 之间的关系(组规模为 $N = 2^k$),如表 1 所示。

由此,在成员具有相同变动概率的多播密钥树的设计时,可以在表 1 中查找出与某多播组中成员变动概率 p 相应的 a 值,确定根结点度数 2^a ,以构造出最优密钥树结构,从而使计算和通信开销最小(这里假设成员变动概率可以预先知晓或计算获得,以下同)。

1.2 成员具有不同变动概率的多播优化树

在实际的多播通信中,同一多播组的成员间的变动概率往往是不同的,这就要求密钥树的组织不能像 1.1 节中成员具有相同变动概率时那样将多播优化树构造为一棵单一的平衡树,而是应该根据成员的行为特性将其分类,每类各自构造其优化子树,以使密钥更

新开销最小。由表 1 可知,当 $0.3 < p < 1$ 时,星型结构密钥更新开销最小,那么将变动概率在此区间的成员(设共 2^{k_1})聚合起来,其密钥树组织为星型结构 T_1 ;当 $0.093 < p < 0.3$ 时, $a = k - 2$ 优化树密钥更新开销最小,那么将变动概率在此区间的成员(设共 2^{k_2})聚合起来,并为其组织一棵根结点度数为 2^{k_2-2} 、中间结点度数为 4、底层结点度数为 2 或 4 的平衡树 T_2 ;依次类推,将符合表 1 中某一区间的成员聚合起来,并构造相应的最优树 T_i 。当然,所有这些子树的根可以为同一个根,如图 1 所示。

表 1 a 和 p 间的关系

a	p
星型	0.3~1
$k-2$	0.093~0.3
$k-3$	0.056~0.092
$k-4$	0.0256~0.055
$k-5$	0.014~0.0255
$k-6$	0.0066~0.013
$k-7$	0.0034~0.0065
$k-8$	0.0017~0.0033
$k-9$	0.00084~0.00160
$k-10$	0.00042~0.00083
$k-11$	0.00021~0.00041
$k-12$	0.00011~0.00020
$k-13$	0.0001
.....

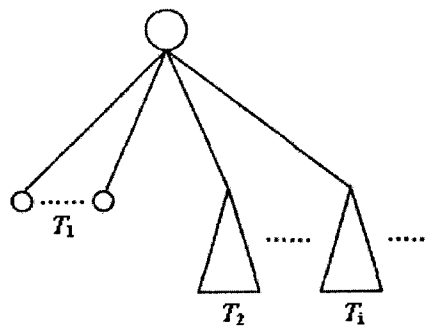


图 1 密钥树的概率组织结构

如果组规模 $N \rightarrow \infty$, 并且可以获得足够精确的成员变动概率,那么子树可以一直细化下去(因为 a 的变化值与 p 的变化值成 2 的指数函数关系)。考虑到密钥树的简化,对于 $0 < p < 0.01$ 的情况,可以用一棵 a 取较小值的优化树统一表示。因为实际多播组(规模 N 一般不会超过 2^{30})中处于这一区间的成员很少,而且由经验知当 $0 < p < 0.01$ 时, a 取值小于最优值时,密钥更新开销增量很小,另外,获得高精度度的成员变动概率也有困难,所以简化树更能提高多播性能,减小组

管理者的负担。综上所述,图 1 可以简化为包含 T_1 , T_2, T_3, T_4, T_5, T_6 的密钥树(T_6 一般取 $a_1 = 1, 2$ 的优化树),即简化的概率优化树。

2 算法与仿真实验

2.1 算法设计

根据以上对密钥树的概率组织方法的研究,可以发现构造成员具有相同变动概率的多播优化树其实是构造成员具有不同变动概率的多播优化树的一种特例。对于一般的多播组,构造简化的概率优化树,其算法如下:

每个密钥更新周期到达时,

(1)获取(或计算)新加入成员的变动概率。

(2)根据其变动概率将新加入成员分为 6 类: $0.3 \leq p < 1$ 归为 C_1 ; $0.093 \leq p < 0.3$ 归为 C_2 ; $0.056 \leq p < 0.093$ 归为 C_3 ; $0.0256 \leq p < 0.056$ 归为 C_4 ; $0.01 \leq p < 0.0256$ 归为 C_5 ; $0 < p < 0.01$ 归为 C_6 。

(3)insert(T_i, C_i)。如果 C_i 中的成员数小于等于 T_i 中离开成员数和空闲叶结点之和,直接将 C_i 中的新成员插入到 T_i 中;如果 C_i 中的成员数大于 T_i 中离开成员数和空闲叶结点之和,则根据平衡优化树构造方式重新构造 T_i 。

(4)更新密钥。

2.2 仿真实验及分析

实验假设多播组处于一个相对稳定的状态,计算组的批量密钥更新开销,即 T_i 中的成员数相对稳定,不需要考虑重新构造 T_i 的开销,只考虑管理者的加密次数(E)。假设组规模 $N = 2^k, k \in [10, 30]$,实验对采用概率优化树方式的管理者密钥更新开销与采用二叉树、四维树以及星型结构方式的密钥更新开销进行了

比较(如图 2 和图 3 所示)。

实验一:假设所有成员的变动概率符合均匀分布,比较采用星型结构、二叉树、四维树以及密钥树概率组织方法时管理者的批量密钥更新开销。

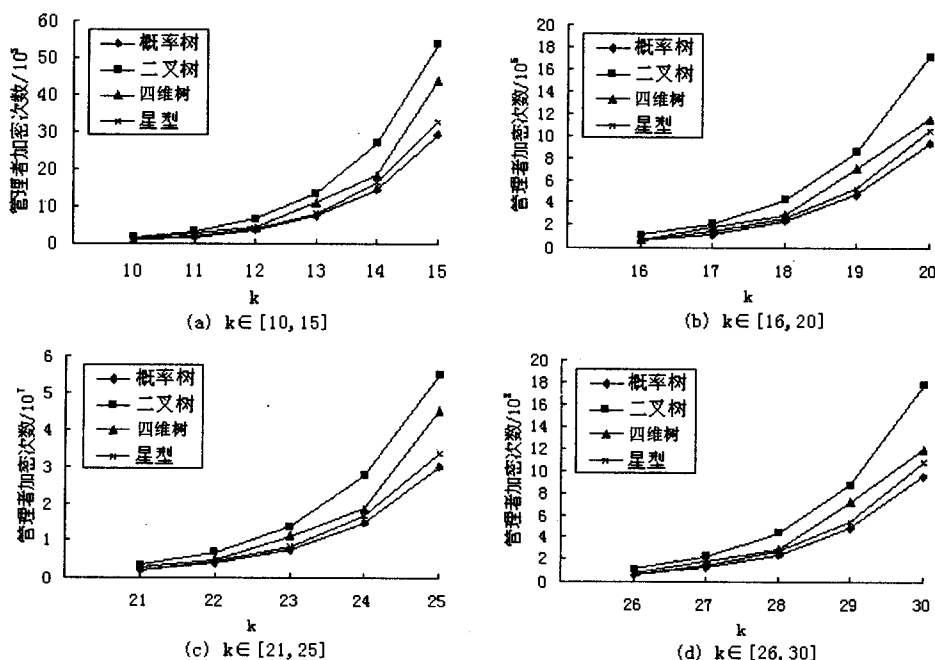


图 2 实验一时四种密钥组织结构比较

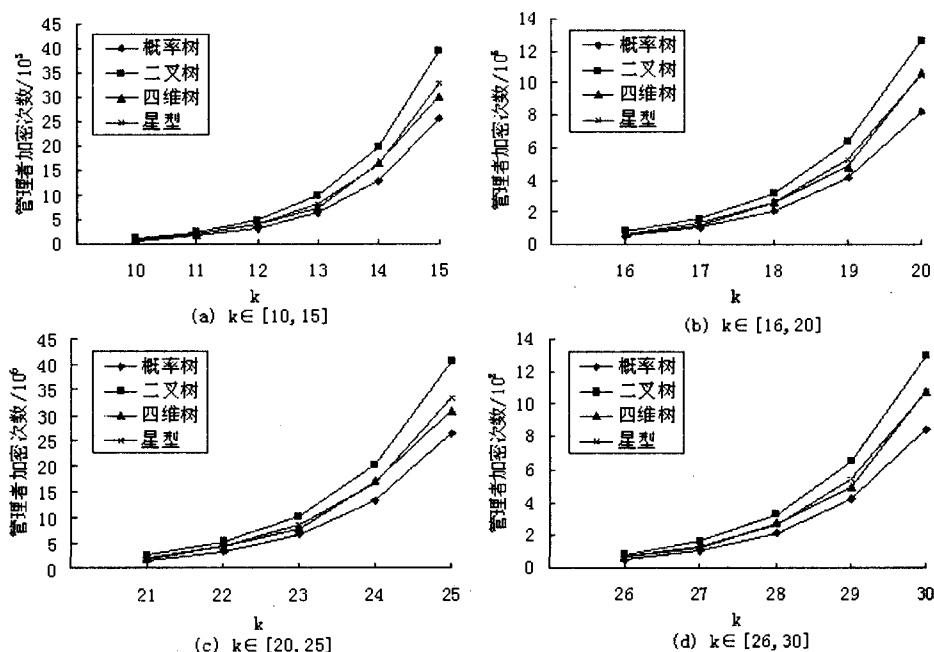


图 3 实验二时四种密钥组织结构比较

图 2(a) 中绘制了 k 取 $[10, 15]$ 时四种密钥组织结构各自的 \bar{E} (管理者的平均加密次数)。图 2(b) ~ (d) 则分别绘制了 k 取 $[16, 20]$ 、 $[21, 25]$ 、 $[26, 30]$ 时的情况。如图所示,无论 k 取何值,概率优化树均优于其它三种密钥组织结构。在一次批量密钥更新中,其平均加密次数比星型结构减少 11%,比二叉树减少 45.5%,

比四维树减少 19.46% (为偶数)、33.5% (为奇数)。另外,概率树、二叉树、星型结构其加密次数均随着 k 的增长呈 2 倍增长;而四维树其加密次数随着 k 的奇数(或偶数)增长呈 4 倍增长。

文献[7]中指出成员在某些多播组中或者停留极短的时间或者待满整个多播会话过程。故假设有一半成员属于 C_1 ,即在星型结构中,而另一半成员处于其它子树中。

实验二:假设 $N/2$ 成员属于 C_1 , $N/4$ 成员属于 C_2 , $N/8$ 成员属于 C_3 , $N/16$ 成员属于 C_4 , $N/32$ 成员属于 C_5 , $N/64$ 成员属于 C_6 ,比较上述四种密钥组织结构在批量密钥更新时管理者的密钥更新开销。

图 3(a)~(d)分别绘制了 k 取[10,15]、[16,20]、[21,25]、[26,30]时四种密钥组织结构各自的 \bar{E} 。如图所示,无论 k 取何值,概率树均优于其它三种密钥组织结构。在一次批量密钥更新中,其平均加密次数比星型结构减少 21%,比二叉树减少 34.8%,比四维树减少 22% (k 为偶数)、14.4% (k 为奇数)。概率树、二叉树、星型结构其加密次数均随着 k 的增长呈 2 倍增长;而四维树其加密次数随着 k 的奇数(或偶数)增长呈 4 倍增长。

综上实验,无论 k 取何值,概率树效率较其它三种密钥组织结构都有较大的优势,尤其是相对于普通的平衡二叉树,显著地减小了管理者的密钥更新开销。

在实验一的条件下,四维树优于星型结构;而在实验二的条件下, k 为奇数时,四维树较好, k 为偶数时,星型结构较好。这也符合表 1 的结果,成员变动概率越大,星型结构越有优势;成员变动概率越小,树型结构越有优势。如果成员变动概率均很大(趋向 1),二叉树的密钥更新开销接近概率树(此时即为星型结构)的 2 倍;如果成员变动概率均很小(趋向 0),星型结构的密钥更新开销接近概率树(此时即为树型结构)的几百倍。

3 结 论

对多播密钥树的组织结构进行理论研究,综合星型结构和树型结构,给出了密钥树的一种概率组织方法,较传统的平衡二叉树显著地减小了密钥更新开销。

概率组织方法的关键是对成员依据其变动概率进行分类,尤其是将属于 C_1 的成员与属于其它类的成员划分开。关于成员变动概率的计算问题,文中没有涉及,是下一步的研究工作。简单的可以用附权值的方法,也可尝试采用赌轮等智能方法进行分类。另外,如果成员的变动概率呈现两极化或大多数成员的变动概率较大时,可以牺牲小部分的效率,将简化树再次简化为两分树的形式——星型结构和 $a = 1, 2$ 的优化树,这在成员变动概率难以获得(或代价过高)时,具有更高的实际意义。

参考文献:

- [1] Wallner D, Harder E, Agee R. Key Management for Multicast: Issues and Architecture [EB/OL]. 1998-09. Internet Draft, ftp://ftp.ietf.org/internet-drafts/draft-wallner-key-arch-01.txt.
- [2] Wong Chung Kei, Gouda M, Simon S. Lam Secure Group Communications Using Key Graphs[J]. IEEE/ACM Transactions on Networking, 2000, 8(1): 16-30.
- [3] Steve L X, Richard Y Y, Gouda M G, et al. Batch Rekeying for Secure Group Communications[C]//Proceedings of the 10th International World Wide Web Conference. Hong Kong, China: [s. n.], 2001: 525-534.
- [4] Zhu F, Chan A, Noubir G. Optimal Tree Structure for Key Management of Simultaneous Join/Leave in Secure Multicast [C]//IEEE Military Communications Conference. Boston: [s. n.], 2003(2): 773-778.
- [5] Selcuk A, McCubbin C, Sidhu D. Probabilistic Optimization of LKH-based Multicast Key Distribution Schemes [EB/OL]. 2000. http://www.ietf.org/internet-drafts/draft-selcuk-probabilistic-lkh-01.txt, Internet Draft.
- [6] Zhu S, Setia S, Jajodia S. Performance Optimizations for Group Key management Schemes for Secure Multicast [C]//Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems. Rhode Island, USA: [s. n.], 2003: 163-171.
- [7] Almeroth K, Ammar M. Multicast Group Behavior in the Internet's Multicast Backbone (MBone) [J]. IEEE Communications Magazine, 1997, 35(6): 224-229.
- [8] 许 勇. 批量密钥更新中密钥组织方法的研究与实现[J]. 东南大学学报: 自然科学版, 2006, 36(3): 488-492.

(上接第 139 页)

傅建明等译. 北京: 电子工业出版社, 2005: 218-227.

- [8] Stinson D R. 密码学原理与实践[M]. 第 2 版. 冯登国译. 北京: 电子工业出版社, 2003: 245-246.
- [9] 徐雷鸣, 庞 博, 赵 耀. NS 与网络模拟[M]. 北京: 人民

邮电出版社, 2003: 1-8.

- [10] Certicom Corp. The Elliptic Curve Cryptosystem [EB/OL]. 1998-03. http://www.certicom.com.