安全多播密钥更新性能分析

李 辉
(河南科技大学,河南 洛阳 471003)

摘 要:随着 Internet 的发展,多播作为面向组应用的一种高效的通信机制被广泛应用。为了提供安全多播,当新成员加入或者成员离开系统,通信加密密钥就必须改变。目前,密钥图的方案已经被提出,其中树形结构密钥图和星型结构是两种重要类型。分析树形结构的密钥图和星形结构的密钥图独立更新方式带来的更新代价.重点分析基于这两种结构批量更新的性能。得出结论:离开和加入请求相对较少时,树形结构有较好的性能,请求较多的情况的星型结构较为适合。

关键词:密钥图;树形结构密钥图;星型结构密钥图;独立更新;批量更新
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)07-0187-04

Analysis of Performance on Rekeying of Multicast Security

LI Hui
(Henan University of Science and Technology, Luoyang 471003, China)

Abstract: With the rapid development of Internet, many emerging Web applications are based on a group communication model. The secure group communication has become an important issue. At present, key graph approach has been proposed for group management. Key tree and key star are two important types of key graph. In the paper, analyzed the individual rekeying on key tree and key star and the server' cost on batch rekeying of key tree and key star. Draw a conclusion that when the number of requests in a batch is not large, key tree is better; otherwise, key star (a special key tree with root degree equal to group size) outperforms small-degree key trees.

Key words: key graph; key tree; key star; individual rekeying; batch rekeying

0 引 言

随着 Internet 的飞速发展,出现了许多基于多播通信模型的 Web 应用。多播提供了一种一个或多个发送点向组中所有成员,高效尽力而为的数据传送机制,因此 安全多播通信将成为一个重要 Internet 问题。

为了进行安全多播通信,一种方法就是多播组成员共享会话密钥即组密钥,组成员用组密钥加密发向组的数据和解密接收到的用组密钥加密的数据。当成员关系发生变化时,及时更新组密钥,保证新加入的成员不能访问加入之前的数据(前向访问控制)和离开成员不能访问离开组以后的数据(后向访问控制)[1]。多播与传统的单播相比,最大特点就是组成员关系随时都可能发生变化即新成员加入和组成员离开多播组。这使得多播组的组密钥的管理变得相当复杂。目前已经提出很多种组密钥的管理方案,如 SKDC(Simple Key Distribution Center)[2]、LKH(Logical Key Hiberarchy)[3]、OFT (One way Function Tree)[4]、SDR(Subset Difference Re-keying)[5],WKA-BKR[6]等,这些管理方案可以大致分成两种类型:树形结构的组密钥管理方案和星型结构的组密钥管理方案。

文中讨论两种类型的密钥图:树形的密钥图和星形的密钥图,并对两种方案的独立更新和批量更新方案进行了性能分析。

1 密钥图

在图中假定密钥图密钥服务器是可信任的、安全的,负责管理密钥。密钥图是一个由 U 节点和 K 节点组成有向无圈图,其中 U 节点代表用户节点,K 节点代表密钥节点。星形和树形的密钥图是密钥图中重要的两种类型。

1.1 星形密钥图

星形密钥图是一种特殊的树形密钥图,根节点的度数等于组成员数。在星形密钥图中,每个用户成员存储两个密钥:用户的私钥和会话密钥即组密钥,根节点代表组密钥。图1(a)是一个有4个用户的星形密钥图。

收稿日期:2008-10-21;**修回日期**:2008-12-30
基金项目:教育部博士点基金资助项目(20070614008)
作者简介:李 辉(1977-),男,河南洛阳人,硕士,研究方向为计算机网络和数据库。

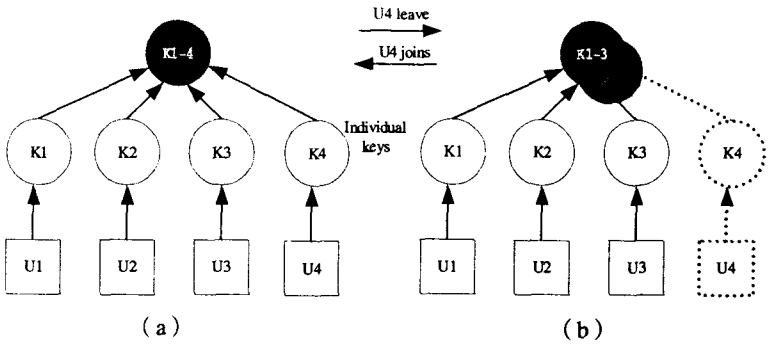

图 1 星形密钥图

当组成员关系发生变化是，要及时更新组密钥保证多播通信的安全性。

当成员 $U4$ 离开多播组(图 1(a)→(b))，密钥服务器用用户的私钥加密新的组密钥 $K1-3$，然后生成密钥更新消息多播到整个组：

$S \rightarrow u1, u2, u3: \{k1-3\}k1, \{k1-3\}k2, \{k1-3\}k3$

当成员 $U4$ 要加入多播组(图 1(b)→(a))，密钥服务器单播 $U4$ 的私钥 $K4$ 给 $U4$，然后用 $K4$ 和原组密钥 $K1-3$ 加密新的组密钥，生成如下密钥更新消息多播到组：

$S \rightarrow u1, u2, u3: \{k1-4\}k1-3$

$S \rightarrow u4: :\{k1-4\}k4$

当成员离开和新用户加入服务器的更新代价分别为 $N-1$ 和 2，其中 N 是多播组成员数。

显然，星形密钥图更新代价和多播系统的规模呈线性关系，有较差的可扩展性。

1.2 树形密钥图

树形密钥图中，U 节点和 K 节点被组织成树形结构，其中根节点是组密钥，叶子节点代表用户节点的私钥，其他的节点代表为了降低更新代价引入的辅助密钥。用户节点持有从组成员对应的叶节点到根节点路径上的所有密钥。图 2(a) 是一个成员数 $N=9$ 的多播组的密钥树，其中树的度 $d=3$，高度 $h=3$。在该逻辑密钥树中位于第 1 层的树根 $K1-9$ 多播组的组密钥，叶子结点 $K1 \sim K9$ 是成员的私钥，而中间节点 $K123, K456, K789$ 是组密钥更新的辅助密钥。多播组中的每个成员持有从对应的叶子节点到达树根时路径的所有密钥，如 $U9$ 持有 $K9$、$K78$、$K1-9$。

当组成员关系发生变化(退出或加入)时，密钥服务器需要更新组密钥及部分辅助密钥以达到机密性要求。成员 $U9$ 要离开多播组(图 2(a)→(b))，密钥服务器需要更新 $U9$ 存储的密钥 $K789$ 为 $K78$，$K1-9$ 为 $K1-8$，然后密钥服务器生成如下更新消息多播到整个组：

$S \rightarrow u1, \cdots u8: \{k78\}k7, \{k78\}k8,$

$\{k1-8\}k123\{k1-8\}k456\{k1-8\}k78$

用户 $U9$ 要加入多播组(图 2(b)→(a))，密钥服务器先为新用户找到一个加入点 $K78$，同时单播新用户 $U9$ 的私钥 $K9$ 给 $U9$，然后把密钥更新消息多播到整个多播组，同时单播用 $K9$ 加密的密钥 $K789$ 和 $K1-9$：

$S \rightarrow u1, \cdots, u9: \{k1-9\}k1-8\{k789\}k78$

$S \rightarrow u9: \{k1-9\ k789\}k9$

采用树形结构密钥图，假定树是完全平衡树，则成

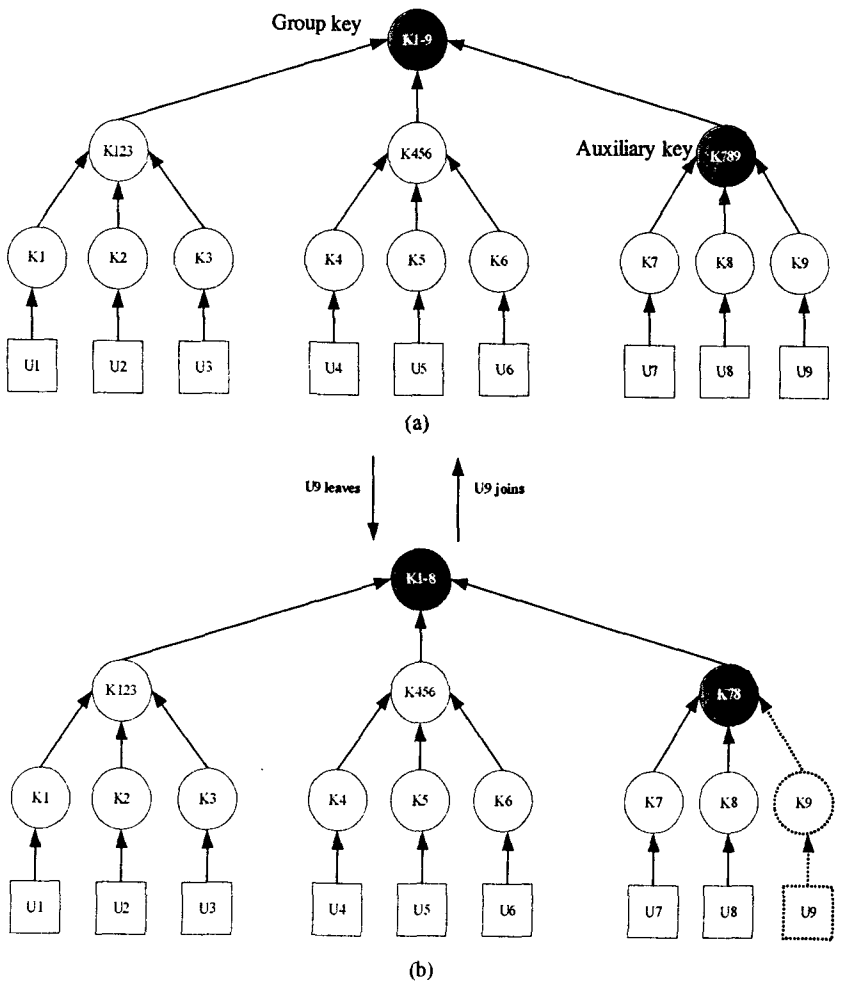

图 2 树形密钥图

员离开的更新代价为 $d\log_d N - 1$,新成员加入的代价为 $2\log_d N$,其中 N 为个用户节点,d 为树的度数,文献[7]表明当 $d = 4$ 是组成员离开的最佳度数。

2 星形和树形密钥图批量性能分析

当成员关系发生变化时,立即更新组密钥的方式,称之为独立更新[8]。理论上独立更新方式保证了多播通信的前、后向安全性[9],然而却带来两个问题:传输延迟带来的密钥与数据的不同步[8],即因传输延迟新密钥不能解密旧密钥加密的数据和旧密钥不能解密新密钥加密的数据与密钥服务器的低效问题。当成员关系发生变化时,不立即更新组密钥而是等一段时间进行更新的方式,称之为批量更新[10],批量更新缓解独立更新方式的不同步和低效问题,但牺牲系统一定的安全性。

2.1 星形密钥图

在星形密钥图中,时间间隔 T 内,假定 J 代表加入组新成员和 L 代表离开组成员,N 是组成员数,采用立即更新的方式服务器密钥更新的代价:

$$R_I(N,J,L) = \begin{cases} 2J & \text{if } L = 0 \\ (N-1)L + 2J & \text{if } L > 0 \end{cases}$$

采用批量更新更新的方式,密钥服务器的代价:

$$R_B(N,J,L) = \begin{cases} J+1 & \text{if } L = 0 \\ N+1-L & \text{if } L > 0 \end{cases}$$

显然,采用批量更新的方式相比立即更新的方式,密钥服务器节省密钥更新的代价,提高密钥服务器的效率。

2.2 树形密钥图

在时间间隔 T 内,树形密钥图采用立即更新的方式密钥服务器的组密钥更新代价:

$$T_I(N,d,J,L) = (dL + 2J)\log_d N - L$$

树形密钥图采用批量更新方式更新代价主要取决于新加入用户节点。分成四种情况进行讨论:

情况 1:$J = L$,用加入新成员替换离开的组成员;

情况 2:$J < L$,在 L 个要离开的节点中找出 J 个较浅的节点用新加入的用户节点替换;

情况 3:$J > L, L = 0$,首先在密钥树中找一个最浅的叶子节点,把 V 从密钥树中删除;然后新加入用户和 V 构造一棵完全树[11],但 T 不一定是平衡;把树 T 放置到 V 原来的位置;

情况 4:$J > L, L > 0$,用 L 个加入节点替换离开的节点,然后 $(J - L)$ 个加入节点按情况 3 处理;

则批量更新的更新代价:

$$T_B(N,d,J,L) = \begin{cases} 2\log_d N + \left\lceil \dfrac{dJ}{d-1} \right\rceil \\ \qquad J > L \text{ and } L = 0 \\ \left\lceil \dfrac{d(J-L)}{d-1} \right\rceil + W_{J=L}(N,d,L,L) \\ \qquad J > L \text{ and } L > 0 \\ W_{J=L}(N,d,L,L) - (L-J) \\ \qquad J > L \\ Ld\log_d \dfrac{N}{L} + \dfrac{d(L-1)}{d-1} \\ \qquad J = J \text{ and } L = d^k \\ d^{k+1}(h-k) + rd(h-k-1) + \dfrac{d(d^k-1)}{d-1} \\ \qquad J = L \text{ and } L = d^k_{+r} \end{cases}$$

3 星形和树形密钥图批量更新的仿真

通过仿真比较星形密钥图和密钥树。图 3 和图 4 分别为星形密钥图和 $N = 1024$ 的 2 度密钥树与星形密钥图和 $N = 4096$ 的 4 度密钥树的批量更新的性能仿真。图中阴影的区域代表星形密钥图性能较好的部分,非阴影的区域是属性密钥图性能较好的部分。

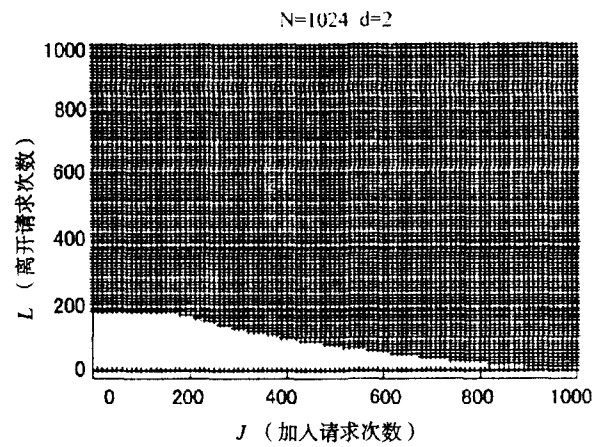

图 3　$N = 1024, d = 2$ 两种密钥图的更新性能仿真

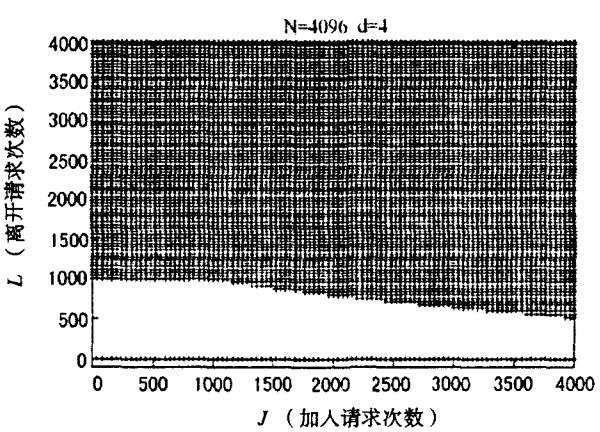

图 4　$N = 4096, d = 4$ 两种密钥图的更新性能仿真

从图中可以看出,当离开成员和加入新成员数量

较大或者离开成员数 $L = 0$ 时，采用星形密钥图有较好的性能，有较小的更新开销。通过图 3 和图 4 可以得出相似的结论，就是当成员离开数 $L < N/4$ 或加入成员数 $J < N/2$ 时，密钥树比星形密钥图有好的性能，更新代价较低；其他的情况，星形密钥图有较好的性能，有低的更新代价。

4 结束语

文中分析树形结构的密钥图和星形结构的密钥图独立更新方式带来的更新代价，重点仿真星形和树形结构批量更新的性能，从而得出一个大致的结论：当成员离开数 $L < N/4$ 或加入成员数 $J < N/2$ 时，采用树形结构有较好的性能，而采用星形结构有较好的更新性能。该结论对实际的应用有一定指导意义，从而降低更新密钥的代价，提高密钥服务器的性能。

参考文献：

[1] Chung Kei Wong, Gouda M, Lam S S. Secure group communications using key graphs[C]//Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication. NY, USA: ACM, 1998:68 - 79.

[2] 许 勇，陈 恺. 安全多播中基于成员行为的 LKH 方法[J]. 软件学报，2005，16(4)：601 - 608.

[3] 蔡延荣，王清贤，李梅林，等. 安全多播密钥更新研究[J]. 计算机技术与自动化，2003，22(3)：110 - 112.

[4] David A, Grew M, Sherman T. Key Establishment in Large Dynamic Groups Using One - Way Function Trees[M]// IEEE Transactions on Software Engineering. NJ, USA: [s. n.], 2003:444 - 458.

[5] Naor D, Naor M, Lotspiech J. Revocation and Tracing Schemes for Stateless Receivers[C]//Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer - Verlag, 2001:41 - 62.

[6] Setia S, Zhu S, Jajodia S. A Scalable and Reliable Key Distribution Protocol for Multicast Group Rekeying[R]. Virginia, US: Department of Information and Software Engineering, George Mason University, 2002:1 - 14.

[7] 李彦希，赵 耀，林 闯，等. 基于单向函数树的高效分布式组密钥管理方案[J]. 清华大学学报：自然科学版，2005，45(10)：1417 - 1420.

[8] 杨焱林. 基于 LKH 混合树的多播密钥更新方案[J]. 现代电子技术，2004，27：31 - 32.

[9] Heydari M H, Morales L, Sudborough I H. Efficient Algorithms for Batch Re - keying Operations in Secure Multicast [C]//Proceedings of the 39th Hawaii International Conference on System Sciences. [s. l.]: [s. n.], 2006.

[10] 屈 劲，葛建华，蒋 铭. 安全多播密钥批更新算法研究[J]. 电子学报，2003，31(7)：1047 - 1048.

[11] 赵 欣，吴敏强，陈道蓄，等. 一个自适应的安全组通信秘钥更新算法[J]. 电子学报，2003，31(5)：656 - 658.

(上接第 183 页)

[6] 李 玮，侯整风. SSL 协议安全缺陷分析[J]. 计算机技术与发展，2006，16(12)：224 - 226.

[7] Dandash O, WU Xiaoping, Le Phu Dung. Wireless Internet Payment System Using Smart Cards[C]// Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05). Nevada: IEEE Computer Society, 2005.

[8] WU Xiaoping, Dandash O, Le Phu Dung. The Design and Implementation of a Smart phone Payment System based on Limited - used Key generation scheme[C]// Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06). [s. l.]: IEEE Computer Society, 2006.

[9] 邢书宝，李 刚，薛惠锋. 一次一密加密系统设计与实现[J]. 计算机技术与发展，2007，17(3)：150 - 152.

(上接第 186 页)

参考文献：

[1] 盛津芳，王 斌，陈松乔. 方面化构件模型及其组装方法[J]. 计算机工程，2006，32(5)：39 - 40.

[2] Hilsdale E, Hugunin J. Advice weaving in aspect[C]//Proc. of the 3rd International Conference on Aspect - Oriented Software Development (AOSD 2004). Lancaster, UK: ACM Press, 2004:26 - 35.

[3] 陈 成，李 行. 基于 AOP 的 MDA 模型转换[J]. 计算机技术与发展，2008，18(7)：87 - 90.

[4] 古全友，王恩波，胥昌胜. AOP 技术在 J2EE 系统构建中的应用[J]. 计算机技术与发展，2006，16(4)：150 - 152.

[5] 钱竹青，邹正武. Eclipse AspectJ——利用 Eclipse 和 AspectJ 进行面向方面程序设计[M]. 北京：清华大学出版社，2006.

[6] Nicholas L. Using AspectJ Enhancing Design Patterns[EB/OL]. 2005. http://www - 128. ibm. com /developerworks/.

[7] 王 斌，周 亮，谭云桥，等. 基于类修改和反射的动态方面编织模型[J]. 计算机工程与应用，2008，44(7)：82 - 85.

[8] SUN. Introduction to JAAS Authorization[EB/OL]. 2002 - 11. http://java. sun. com/j2se/1. 4. 2 /docs/guide/.