基于二分图的组密钥管理方案设计

周 杰 饶艳芬 李慧芬
(华南理工大学广东省计算机网络重点实验室 广州 510641)

摘 要 随着基于群组通信应用的不断发展,安全群组通信成为目前分布式计算领域和信息安全领域研究的一个热点问题。有效的组密钥管理是安全群组通信需要解决的关键问题。将一个安全群组通信系统中组成员拥有的辅助密钥与组成员之间的关系用一个二分图表示,将设计组密钥管理方案问题转化为构造满足一定条件的二分图的问题,为设计组密钥管理方案提供了一种新途径。利用构造的二分图设计了一种组密钥管理方案。所设计的组密钥管理方案不需要组管理中心保存树或矩阵等结构,因而降低了组管理中心的存储开销,另外避免了类似LKH方案中维持平衡树的开销。

关键词 安全群组通信系统,组密钥管理,辅助密钥,二分图
中图法分类号 TP309 **文献标识码** A

Design of Group Key Management Scheme Based on Bipartite Graph

ZHOU Jie RAO Yan-fen LI Hui-fen
(Guangdong Key Laboratory of Computer Network, South China Univ. of Tech., Guangzhou 510641, China)

Abstract With the development of application based on group communication, secure group communication has become a hot topic of current distributed computing and information security field. Efficient group key management is the key problem to be resolved by secure group communication. This paper used a bipartite graph to express the relation between the assistant keys owed by members and members in the secure group communication system, transformed the problem of designing group key management scheme into the problem of constructing a bipartite graph which satisfies certain conditions. This provided a new way to design group key management scheme. The paper designed a group key management with the constructed bipartite graph. There is no need for the scheme to use group center to save trees or matrix. So it can reduce the storage cost of GC(Group Center), and can avoid the cost of keeping balanced tree such as LKH scheme.

Keywords Secure group communication system, Group key management, Assistant key, Bipartite graph

随着互联网技术的发展、网格计算和无线网络的出现,群组通信技术(如IP组播、应用层组播、IP广播等)越来越受到人们的关注[1]。群组通信在视频会议(video conferencing)、视频点播(video on demand)、网络电视(TV over Internet)、软件更新(software updates)、数据库复制(database replication)、广播式股票报价(broadcasting stock quotes)和交互式多方游戏(interactive group games)等业务,以及在军事上都有广泛的应用[1,2]。随着基于群组通信应用的不断发展,安全群组通信成为分布式计算领域和信息安全领域研究的一个热点问题,吸引了众多研究者的关注[1-3]。其中,组密钥的安全管理是安全群组通信的核心问题。在安全群组通信过程中,组成员是动态变化的。当组成员变化时,为了满足前向或后向机密性,需要更新组密钥。为了有效更新组密钥,每个组成员需要持有一个或多个辅助密钥(auxiliary key)[1,9]。如何安全有效地对组密钥和辅助密钥进行管理和更新,是组密钥管理的主要问题[1-3]。

近年来国内外研究者已经提出了许多组密钥管理方案[1]。其中,由Wong等[4]和Wallner等[5]分别独立设计的基于逻辑密钥层次(Logical Key Hierarchy, LKH)树的组密钥管理方案(简称LKH方案)是目前研究较多并被人们普遍接受的性能较优的一种组密钥管理方案。为了进一步优化LKH方案,研究者从不同方面对其进行了改进[6-8]。为了降低安全群组通信系统中组管理中心和组成员存储的辅助密钥的数量以及密钥更新时的计算开销和通信开销,Eltoweissy[9]等给出一种基于组合优化的排除系统的组密钥管理方案。LKH方案及其改进方案都需要组管理中心维护一棵有n(n是组成员数)个叶节点的密钥树;而基于排除系统的组密钥管理方案需要组管理中心维护一个规范矩阵。特别地,每当群组规模增加到一定程度时,必须重新构造规范矩阵。在群组规模很大且组成员资格变动频繁情况下,维护密钥树或规范矩阵的开销是不可忽视的。

本文通过将安全群组通信系统中组成员拥有的辅助密钥

到稿日期:2008-05-15 本文受国家973计划项目(2003CB314805),国家CNGI项目(CNGI-04-13-2T)资助。
周 杰(1964—),男,副教授,博士,主要研究方向为高性能网络技术、信息安全,E-mail:jiezhou@scut.edu.cn;饶艳芬(1979—),女,研究生;李慧芬(1983—),女,研究生。

与组成员之间的关系用一个二分图表示，将设计组密钥管理方案问题转化为满足一定条件的二分图的构造问题。从不同角度给出了组密钥管理方案的设计方法，为设计组密钥管理方案提供了一种新途径。利用构造的二分图设计了一种组密钥管理方案。所设计的组密钥管理方案不需要组管理中心保存树或矩阵等结构，因而降低了组管理中心的存储开销，也避免了类似 LKH 方案中维持平衡树的开销。

1 用二分图表示组成员与辅助密钥的关系

在一个安全群组通信系统中，为了在组成员变化时更新组密钥，每个组成员需要持有一个或多个辅助密钥。同时，一个辅助密钥也可能由一个或多个组成员拥有。组成员与所持有的辅助密钥之间的关系可用一个二分图表示。

例如，在 LKH 方案中[4,5]，组成员所持有的组密钥和辅助密钥构成一棵有 n(n 为组成员数)个叶子结点的密钥树 T，并由组管理中心保存。密钥树根结点的密钥为组密钥，其它结点的密钥为辅助密钥。每个组成员对应一个叶结点。每个组成员与组管理中心共享从其对应的叶结点到根结点路径上的每个结点的密钥(除根结点的密钥外，路径上其它结点密钥均为该组成员的辅助密钥)。图 1 所示为有 6 个组成员的密钥树 T。结点 U_1 与组管理中心共享密钥$\{GK,K_1,K_2,K_5\}$，结点 U_2 与组管理中心共享密钥$\{GK,K_1,K_2,K_6\}$等等。

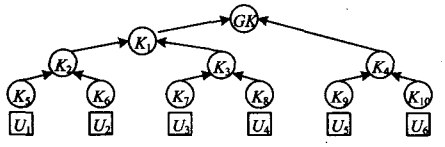

图 1 LKH 树

LKH 方案中，组成员与所持有的辅助密钥之间的关系可用一个二分图表示。图 1 所示的密钥树中，组成员拥有的辅助密钥和组成员之间的关系由图 2 所示的二分图表示。

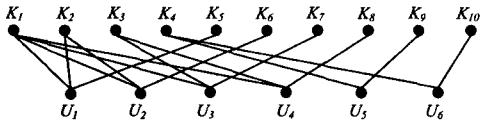

图 2 LKH 方案中表示组成员与所持辅助密钥之间关系的二分图

当安全群组通信过程中有组成员加入或离开时，通过二分图可确定需要更新的辅助密钥，并根据该二分图设计辅助密钥和组密钥的更新方法。例如，在图 2 中，当组成员 U_2 离开群组时，组管理中心可删除辅助密钥 K_2 和 K_6，更新辅助密钥 K_1(设更新后的密钥仍记为 K_1)和组密钥 GK。组管理中心用 K_3 和 K_5 分别加密更新后的 K_1，发送给组成员 U_3，U_4 和 U_1；用更新后的 K_1 和辅助密钥 K_4 加密更新的组密钥 GK'，发送给剩余的组成员。假设在某时刻被删除的 U_2 或一个新的组成员(仍记为 U_2)加入群组，设组成员 U_2 加入后的组成员与所持辅助密钥之间关系的二分图仍为图 2，此时需要产生和更新辅助密钥 K_6，K_1 和 K_2。组管理中心通过安全方式将新的辅助密钥 K_6 发送给 U_2；用 K_5 和 K_6 加密新的辅助密钥 K_2，发送给组成员 U_1 和 U_2；用 K_2 和 K_3 加密更新后的辅助密钥 K_1，发送给 U_1，U_2，U_3 和 U_4；用更新后的 K_1 和辅助密钥 K_4 加密更新的组密钥 GK'，发送给所有组成员。值得注意的是，上述过程需要组管理中心保存二分图结构。下一节将看到，通过构造特定结构的二分图，不需要组管理中心保存二分图结构就可实现组成员加入或退出时的密钥更新。

又如，基于排除系统的组密钥管理方案中[9]，设 n 是安全群组通信系统中的组成员数，k 表示每个组成员存储的辅助密钥的数目，m 是当一个组成员加入或离开群组进行密钥更新时组管理中心需要发送的消息数目。在给定 n 的情况下，为设计具有给定 k 和 m 值的组密钥管理方案，Eltoweissy 等给出排除系统(Exclusion Basis Systems，EBS)概念[9]：

设 $1<k,m<n$，一个排除系统(记为 $EBS(n,k,m)$)是由整数集合$\{1,2,\cdots,n\}$的子集组成的子集族 Γ。对任意 $t\in\{1,2,\cdots,n\}$，满足：

(1) t 至多包含在 Γ 的 k 个子集中；

(2) 恰好存在 Γ 中的 m 个子集 $A_1,A_2,\cdots,A_m$，使得 $A_1\cup A_2\cup\cdots\cup A_m=\{1,2,\cdots,n\}-\{t\}$。

例如，$EBS(8,3,2)$排除系统为：$\Gamma=\{A_1=\{5,6,7,8\},A_2=\{2,3,4,8\},A_3=\{1,3,4,6,7\},A_4=\{1,3,4,5,7\},A_5=\{1,2,3,5,6,8\},\}$。

利用排除系统构造组密钥管理方案，设安全群组通信系统中的 n 个组成员分别从 1 到 n 编号，Γ 中的每个子集对应一个辅助密钥，由组管理中心和该子集所包含的所有组成员共享。因此，组管理中心存储 $|\Gamma|$ 个密钥，每个组成员最多存储 k 个密钥。根据排除系统定义的第 2 条件，当一个组成员加入或离开群组时进行密钥更新，组管理中心需要 m 次加密运算并发送 m 个消息。

基于排除系统 $EBS(8,3,2)$构造的组密钥管理方案中，组成员拥有的辅助密钥和组成员之间的关系可用图 3 所示的二分图表示。同样，当安全群组通信过程中有组成员加入或离开时，通过二分图可确定需要更新的辅助密钥并根据该二分图设计辅助密钥和组密钥的更新方法。

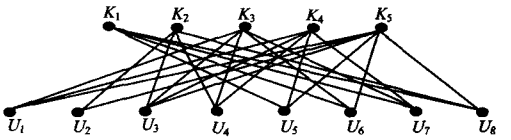

图 3 基于排除系统的组密钥管理方案中表示组成员与所持辅助密钥之间关系的二分图

组密钥管理方案中，组成员与所持辅助密钥之间的关系表示为一个二分图。反之，给定一个满足一定条件的二分图，就确定了一个安全群组通信系统中组成员与辅助密钥的关系。当安全群组通信过程中有组成员加入或离开时，通过二分图可确定需要更新的辅助密钥，设计适当的辅助密钥和组密钥的更新过程，进而给出合适的组密钥管理方案。

2 基于二分图构造组密钥管理方案

本节构造一类特殊结构的二分图，基于构造的二分图设计组密钥管理方案。

2.1 二分图确定的组成员和辅助密钥的关系

设二分图 G 的结点集为 $X=\{k_0,k_1,\cdots,k_{n-1},k_m,k_{m+1},\cdots,k_{m+n-1}\}$和 $Y=\{U_0,U_1,\cdots,U_{n-1}\}$。结点集 X 中的元素既表示二分图的结点，也表示相应结点对应的辅助密钥，称为辅助密钥结点；结点集 Y 中的元素表示组成员，称为组成员结点，元素的下标为组成员标号。这里 m 为一个充分大的整数，是为群组规模的扩大而预先设定的。给定一个正整数 l，$l<n$(2.4 节将讨论 l 和 n 之间的关系)。设组密钥管理方案

中每个组成员持有的辅助密钥数为 $l+1$。二分图中与任意组成员结点 U_i 邻接的辅助密钥结点为：k_i，$k_{(i+1) \bmod n}$，…，$k_{(i+l-1) \bmod n}$，k_{m+i}，即 (U_i, k_i)，$(U_i, k_{(i+1) \bmod n})$，…，$(U_i, k_{(i+l-1) \bmod n})$，$(U_i, k_{m+i})$ 为二分图 G 中与结点 U_i 关联的边，$i=0,1,\cdots,n-1$。图 4 是 $n=5, l=3, m=100$ 的二分图。由如上二分图的构造可知，组成员 U_i 持有的辅助密钥为 $\{k_i, k_{(i+1) \bmod n}, \cdots, k_{(i+l-1) \bmod n}, k_{m+i}\}$，$i=0,1,\cdots,n-1$。组管理中心保存所有辅助密钥 $\{k_0, k_1, \cdots, k_{n-1}, k_m, k_{m+1}, \cdots, k_{m+n-1}\}$ 及其编号。在组密钥管理方案中，组管理中心与每个组成员共享其持有的辅助密钥。

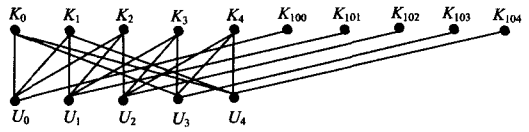

图 4　二分图

2.2　组成员加入

假设当前安全群组通信系统中有 $n-1$ 个组成员，编号为 $0,1,\cdots,n-2$。设经过组管理中心准入控制，一个新组成员加入群组通信，组管理中心将该组成员编号为 $n-1$。组管理中心为组成员 U_{n-1} 生成辅助密钥 k_{m+n-1}，并通过安全方式将 k_{m+n-1} 发送给 U_{n-1}（如通过智能卡等）。组管理中心产生一个新的辅助密钥 k_{n-1}，并分别用 $k_{m+n-l}, k_{m+n-l+1}, \cdots, k_{m+n-1}$ 加密 k_{n-1} 后发送给 $U_{n-l}, U_{n-l+1}, \cdots, U_{n-1}$。组管理中心更新辅助密钥 $k_0, k_1, \cdots, k_{l-2}$（设更新后的辅助密钥仍记为 $k_0, k_1, \cdots, k_{l-2}$）。然后，分别用 $k_m, k_{m+1}, \cdots, k_{m+j}, k_{m+n-l+j+1}, k_{m+n-l+j+2}, \cdots, k_{m+n-1}$ 加密 k_j 后发送给 $U_0; U_1, \cdots, U_j, U_{n-l+j+1}, U_{n-l+j+2}, \cdots, U_{n-1}$，$j=0,1,\cdots,l-2$。最后，组管理中心产生一个新的组密钥 GK'，并分别用辅助密钥 $k_{n-1}, k_{n-1-l}, k_{n-1-2l}, \cdots, k_{n-1-\left[\frac{n-1}{l}\right]l}$（这里 $\left[\frac{n-1}{l}\right]$ 表示 $\frac{n-1}{l}$ 的整数部分）加密 GK' 后发送给相应组成员。图 5 是图 4 对应的二分图中组成员 U_5 加入组播组后的情形，图中虚线是变动或增加的组成员和辅助密钥的关系。

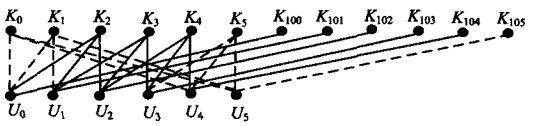

图 5　二分图

由以上过程可以看出，在安全群组通信过程中，当一个新组成员加入到一个已经含有 $n-1$ 个组成员的安全群组通信系统时，组管理中心共需要产生或更新 $l+1$ 个辅助密钥和 1 个组密钥。为了更新辅助密钥需要 l^2 次加密运算，为了更新组密钥需要 $\left[\frac{n-1}{l}\right]+1$ 次加密运算。以一个密钥的长度作为通信量的单位，更新辅助密钥和组密钥的通信量为 $l^2+\left[\frac{n-1}{l}\right]+1$。

2.3　组成员离开

假设当前安全群组通信系统中已有 $n+1$ 个组成员，编号为 $0,1,\cdots,n-1,n$。设在安全群组通信过程中，组成员 U_i $(0 \leqslant i \leqslant n)$ 离开群组。组管理中心将组成员总数减少 1，在辅助密钥列表中删除辅助密钥 k_i 和 k_{m+i}，并向组成员通告离开群组的组成员编号 i。组管理中心和组成员 $U_{i+1}, U_{i+2}, \cdots, U_{n-1}, U_n$ 将相应组成员编号减少 1（若 $i=n$ 则所有剩余组成员编号不改变），即组成员 U_{i+j} 的编号变为 $i+j-1$，组成员标识变为 U_{i+j-1}，$j=1,2,\cdots,n-i$。组管理中心和更改编号后的组成员 $U_i, U_{i+1}, \cdots, U_{n-1}$ 将持有的相应辅助密钥 $k_{i+1}, k_{i+2}, \cdots, k_n$ 和 $k_{m+i+1}, k_{m+i+2}, \cdots, k_{m+n}$ 的编号减少 1（若 $i=n$，则不需要改变辅助密钥编号），即这些辅助密钥的编号分别更改为 $k_i, k_{i+1}, \cdots, k_{n-1}$ 和 $k_{m+i}, k_{m+i+1}, \cdots, k_{m+n-1}$。这样处理的目的是使组管理中心保存的组成员和所持辅助密钥的关系式的形式不变，同时为以后的组成员加入和退出做准备。组管理中心将更改编号后的辅助密钥 $k_{i \bmod n}, k_{(i+1) \bmod n}, \cdots, k_{(i+l-2) \bmod n}$（已离开的组成员所持有的辅助密钥，$i$ 为离开组成员的编号）进行更新，设更新后的辅助密钥仍记为 $k_{i \bmod n}, k_{(i+1) \bmod n}, \cdots, k_{(i+l-2) \bmod n}$。组管理中心分别用 $k_{m+(j-l+1) \bmod n}, k_{m+(j-l+2) \bmod n}, \cdots, k_{m+(j-1) \bmod n}, k_{m+j \bmod n}$ 加密 k_j 后发送给组成员 $U_{(j-l+1) \bmod n}, U_{(j-l+2) \bmod n}, \cdots, U_{j \bmod n}$，$j=i \bmod n, (i+1) \bmod n, \cdots, (i+l-2) \bmod n$。最后，组管理中心产生一个新的组密钥 GK'，并分别用 $k_{n-1}, k_{n-1-l}, k_{n-1-2l}, \cdots, k_{n-1-\left[\frac{n-1}{l}\right]l}$ 加密 GK' 后发送给所有组成员。

由如上过程可以看出，在安全群组通信过程中，当一个组成员离开一个含有 $n+1$ 个组成员的安全群组通信系统时，组管理中心共需要更新 $l-1$ 个辅助密钥和 1 个组密钥，为更新辅助密钥需要 $l(l-1)$ 次加密运算，为更新组密钥需要 $\left[\frac{n-1}{l}\right]+1$ 次加密运算。以一个密钥的长度作为通信量的单位，更新辅助密钥和组密钥的通信量为 $l(l-1)+\left[\frac{n-1}{l}\right]+1$。

2.4　组成员数和组成员所持辅助密钥数之间的关系

设组密钥管理方案中组成员数为 n。首先讨论组成员加入或离开安全群组通信时更新辅助密钥和组密钥的开销的最优值。由 2.2 节和 2.3 节的讨论，为了便于分析，假设组成员加入或离开安全群组通信时为更新辅助密钥和组密钥需要的加密运算次数近似为 $l^2+\left[\frac{n}{l}\right]$。为此，考虑函数 $f(l)=\frac{n}{l}+l^2$。$f(l)$ 在 $l=\left(\frac{n}{2}\right)^{\frac{1}{3}}$ 时取最小值。因此，对于给定的组成员数 n，若组成员和辅助密钥的关系由 2.1 节中给出的二分图确定，在上面的假设下，当组成员持有的辅助密钥数 $l=\left[\left(\frac{n}{2}\right)^{\frac{1}{3}}\right]$，组成员加入或离开群组时更新辅助密钥和组密钥所需的加密运算开销最小。因此，随着组成员数的变化，为使更新辅助密钥和组密钥所需的加密运算开销达到最优，组成员所持的辅助密钥的数量要随着组成员数的变化而改变。

由 $l=\left(\frac{n}{2}\right)^{\frac{1}{3}}$ 得，$n=2l^3$。为了优化更新辅助密钥和组密钥所需的加密运算开销，取组成员数为 $2l^3$ 和 $2(l+1)^3$ 的中间点，即取 $n=2l^3+\frac{2(l+1)^3-2l^3}{2}=l^3+(l+1)^3$，作为组成员持有辅助密钥数量的转换点。假设安全群组通信系统中至少有 4 个组成员。当组成员数 $4 \leqslant n < 9$ 时，每个组成员持有 3 个辅助密钥；当 $l \geqslant 2$，组成员数 n 满足 $(l-1)^3+l^3 \leqslant n <$

$l^3+(l+1)^3$ 时，组成员持有 $l+1$ 个辅助密钥。所以，在安全群组通信过程中组成员加入或退出群组后，当变化后的组成员数 $n\leqslant(l-1)^3+l^3-1$ 时，可将组成员所持辅助密钥数减少1；当变化后的组成员数 $n\geqslant l^3+(l+1)^3$ 时，可将组成员所持辅助密钥数增加1。

2.5 组成员所持辅助密钥数的更改

设当前安全群组通信系统中有 n 个组成员，每个组成员持有的辅助密钥数量为 $l+1$，这里 $(l-1)^3+l^3\leqslant n<l^3+(l+1)^3$。当一个新的组成员加入群组时，若此时组成员数仍满足 $(l-1)^3+l^3\leqslant n+1<l^3+(l+1)^3$，则按照2.2节给出的方法更新辅助密钥和组密钥。若 $n+1\geqslant l^3+(l+1)^3$，则组管理中心首先按照2.2节给出的方法更新辅助密钥和组密钥，然后用 k_{m+i} 加密 $k_{(i+l) \bmod n}$ 后发送给组成员 U_i，$i=0,1,\cdots,n$。这样，每个组成员持有的辅助密钥数增加1。组管理中心将 l 更新为 $l+1$。

由此，当安全群组通信系统中有 $n+1$ 个组成员时，为了使组成员持有的辅助密钥数增加1，需要组管理中心进行 $n+1$ 次加密运算并发送 $n+1$ 个消息。

假设当前安全群组通信系统中已有 $n+1$ 个组成员。设在安全群组通信过程中，组成员 U_i $(0\leqslant i\leqslant n)$ 离开群组。若此时组成员数仍满足 $(l-1)^3+l^3\leqslant n<l^3+(l+1)^3$，则按照2.3节给出的方法更新辅助密钥和组密钥。若 $n\leqslant(l-1)^3+l^3-1$，组管理中心将组成员总数减少1，在辅助密钥列表中删除辅助密钥 k_{m+i}，并向组成员通告离开群组的组成员编号 i。组管理中心和组成员 $U_{i+1},U_{i+2},\cdots,U_{n-1},U_n$ 将相应组成员编号减少1(若 $i=n$，则所有剩余组成员编号不改变)，即组成员 U_{i+j} 的编号变为 $i+j-1$，组成员标识变为 U_{i+j-1}，$j=1,2,\cdots,n-i$。组管理中心重新产生辅助密钥 $k_0,k_1,\cdots,k_{n-1}$，用 k_{m+j} 加密 k_j，$k_{(j+1) \bmod n},\cdots,k_{(j+l-2) \bmod n}$ 后发送给组成员 U_j，$j=0,1,\cdots,n-1$。这样，每个组成员持有的辅助密钥数减少1。组管理中心产生一个新的组密钥 K'，并分别用 k_{n-1}，$k_{(n-1)-(l-1)},k_{(n-1)-2(l-1)},\cdots,k_{n-1-\left[\frac{n-1}{l-1}\right](l-1)}$ 加密 K' 后发送给所有组成员。组管理中心将 l 变为 $l-1$。

由此，当安全群组通信系统中有 n 个组成员时，每个组成员持有的辅助密钥数量为 $l+1$。为了使每个组成员持有的辅助密钥数减少1，需要组管理中心进行 $n(l-1)$ 次加密运算，并发送 n 个消息，每个消息的长度为密钥长度的 $l-1$ 倍。

如上分析可知，更改组成员所持辅助密钥数的开销是很大的，特别是在减少组成员所持辅助密钥数的情况下。因此，如果安全群组通信系统中组成员的规模相对稳定，可采取使组成员持有固定数目辅助密钥的策略，以避免更改组成员所持辅助密钥数的开销。例如，若安全群组通信系统中组成员数稳定在10000到20000之间，可采取使每个组成员持有19个辅助密钥的策略。

3 性能分析

由基于二分图构造的组密钥管理方案可以看出，在方案的设计中二分图只是起辅助作用，组管理中心和组成员并不保存二分图的结构。组管理中心只需保存组成员编号、辅助密钥及其编号，每个组成员只需保存相应的辅助密钥及其编号。在安全群组通信过程中，有组成员加入或退出群组需要更新辅助密钥时，组管理中心只需根据加入或退出的组成员编号，确定需要重新产生或删除的辅助密钥、需要更新的辅助密钥以及用来加密更新后的辅助密钥和组密钥的辅助密钥。与LKH方案和基于排除系统的组密钥管理方案相比，不需要组管理中心保存树或矩阵等结构，从而也避免了类似LKH方案中维持平衡树的开销和基于排除系统的维护规范矩阵的开销。

2.2节和2.3节分析了安全群组通信过程中组成员加入或退出群组时更新辅助密钥和组密钥的计算开销和通信开销。表1是本文给出的方案和LKH方案更新辅助密钥和组密钥的开销以及辅助密钥的存储开销的对比，其中 l 是组成员持有的辅助密钥数。根据2.4节的分析，本文所给的方案中，当 $l=\left[\left(\frac{n}{2}\right)^{\frac{1}{3}}\right]$ 时，组成员加入或离开群组更新辅助密钥和组密钥所需的加密运算次数接近最低。此时，组成员加入群组时更新辅助密钥和组密钥所需的加密运算次数约为 $3\left[\left(\frac{n}{2}\right)^{\frac{2}{3}}\right]$，组成员退出群组时更新辅助密钥和组密钥所需的加密运算次数约为 $3\left[\left(\frac{n}{2}\right)^{\frac{2}{3}}-\left(\frac{n}{2}\right)^{\frac{1}{3}}\right]$。由表1可知，在不考虑更改组成员所持辅助密钥数的情况下，本文所给方案中，组管理中心存储辅助密钥的开销与LKH方案相当，但组成员加入或退出群组时更新辅助密钥及组密钥的计算开销和通信开销以及组成员存储辅助密钥的开销都略高于LKH方案。

表1 与LKH方案的性能对比

	更新辅助密钥和组密钥的开销		辅助密钥的存储开销	
	组成员加入	组成员离开	组管理中心	组成员
LKH方案	$2\log_2(n)$	$2\log_2(n)$	$2n-2$	$\log_2(n)$
本文给出的方案	$l^2+\left[\frac{n-1}{l}\right]+1$	$l(l-1)+\left[\frac{n-1}{l}\right]+1$	$2n$	$l+1$

结束语 通过将一个安全群组通信系统中组成员拥有的辅助密钥与组成员之间的关系用一个二分图表示，将设计组密钥管理方案问题转化为构造满足一定条件的二分图的问题。利用构造的二分图设计了一种组密钥管理方案。

本文给出构造组密钥管理方案的一个新途径。所设计的组密钥管理方案中，不需要组管理中心保存树或矩阵等结构，也避免了类似LKH方案中维持平衡树的开销。

参考文献

[1] Challal Y, Seba H. Group Key Management Protocols: A Novel Taxonomy. International Journal of Information Technology, 2005, 2(1): 105-118

[2] Pham T, Watters P. The Efficiency of Periodic Rekeying in Dynamic Group Key Management // Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07). IEEE: Computer Society, 2007: 425-432

[3] Rafaeli S, Hutchison D. A survey of key management for secure group communication. ACM Computing Surveys, 2003, 35(3): 309-329

[4] Wong C K, Gouda M, Lam S S. Secure Group Communications Using Key Graphs. IEEE/ACM Transactions on Networking, 2000, 8(1): 16-30

(下转第124页)

·物理层模型不考虑捕获问题，在接收节点的传输覆盖范围内，如果有两个以上的发送节点同时发送，则导致接收节点处发生碰撞和传输失败；

·网络节点使用相同的路由协议，不考虑多种路由策略混合使用的问题。

仿真中我们将节点的通信半径依次设置为 150 米、175 米、200 米、225 米、250 米和 300 米。网络中节点使用的路由策略是 MFR 和 NFP[14,15]，在 MFR 策略下，节点在转发分组的时候，倾向于选择距离自己较远的邻节点作为自己的下一跳转发节点；在 NFP 策略下则相反。

统计的指标为节点平均一跳吞吐量，即单位时间内每个节点能够接入信道并成功进行传输的时间片段所占比例的平均值。仿真结果如图 4 和图 5 所示。

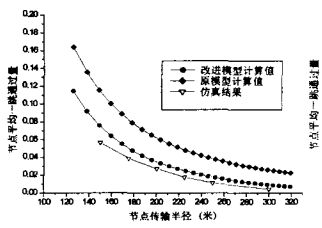

图 4 MFR 路由策略下节点一跳吞吐量

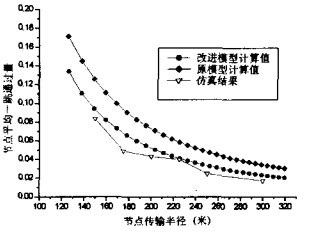

图 5 NFP 路由策略下节点一跳吞吐量

从图中看到，在网络饱和的条件下，原分析模型计算出的节点平均吞吐量明显高于实际的仿真结果。这是因为原模型中的对于传输成功条件的分析过于宽松，它认为只要 RTS/CTS 握手成功，就能成功地预约信道，并保证后续的 DATA/ACK 帧交换成功。实际上，在多跳网络中，如果虚拟载波监听机制失效，接收节点独占区域中的节点是有可能造成 DATA 帧碰撞而导致传输失败的，因此该分析模型高估了 802.11 DCF 在多跳网络中的性能。

在我们的新模型中修改了这一缺陷。从仿真结果可以看出，在两种路由策略条件下，使用新模型分析得到的结果与仿真结果更加接近，准确性有了明显提高。

结束语 本文提出了一种改进的多跳环境下的 IEEE 802.11 DCF 分析模型，它是在原模型基础上，对传输成功条件进行了更为严格的约束后推导得到的。仿真验证结果表明，新模型具有更好的精确性，因而使用该模型所做的研究对实际 Ad Hoc 网络的分析、设计和优化工作具有很好的指导意义。

参 考 文 献

[1] Crow B P. Performance Evaluation of the IEEE 802.11 Wireless Local Area Network Protocol[D]. Tucson: Univ. Arizona, 1996

[2] Weinmiller J, Schlager M, Festag A, et al. Performance Study of Access Control in Wireless LANs IEEE 802.11 DFWMAC and ETSI RES 10 HIPERLAN[J]. Mobile Networks and Application, 1997, 2(2): 55-67

[3] Chhaya H S, Gupta S. Performance Modeling of Asynchronous Data Transfer Methods of IEEE 802.11 MAC Protocol[J]. Wireless Networks, 1997, 3(3): 217-234

[4] Ho T S, Chen K C. Performance Evaluation and Enhancement of the CSMA/CA MAC Protocol for 802.11 Wireless LAN's[A]//Proc. of IEEE PIMRC[C]. Taipei: IEEE Press, 1996: 392-396

[5] Cali F, Conti MGregori E. IEEE 802.11 wireless LAN: Capacity analysis and protocol enhancement[A]//Proc. of INFOCOM'98[C]. San Francisco: IEEE Press, 1998

[6] Bianchi G, Fratta L, Oliveri M. Performance Analysis of IEEE 802.11 CSMA /CA Medium Access Control Protocol[A]//Proc. of IEEE PIMRC[C]. Taipei: IEEE Press, 1996: 407-411

[7] Bianchi G. Performance Analysis of the IEEE 802.11 Distributed Coordination Function[J]. IEEE Journal on Selected Area in Comm., 2000, 18(3): 103-112

[8] Bianchi G. IEEE 802.11 Saturation Throughput Analysis[J]. IEEE Comm. Letters, 1998, 2(12): 13-15

[9] Wu Haitao, Peng Yong, Long Keping, et al. Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancement[A]//Proc. of INFOCOM 2002[C]. IEEE Press, 2002: 599-607

[10] Gupta P, Kumar P R. The capacity of wireless networks[J]. IEEE Transactions on Information Theory, 2000, 46(2): 388-404

[11] Fang Y, McDonald A B. Theoretical Channel Capacity in Multihop Ad Hoc Networks. Local and Metropolitan Area Networks[A]//Proc. of LANMAN 2004[C]. IEEE Workshop. 2004: 181-186

[12] Farshid A S, Suresh S. Analytical Models for Single - Hop and Multi-Hop Ad Hoc Networks[A]//Proceedings of the First International Conference on Broadband Networks (BROADNETS'04)[C]. IEEE Press, 2004: 412-417

[13] 刘凯，李建东，章欣. 多跳移动分组无线网络的吞吐率分析[J]. 西安电子科技大学学报，2000，27(1)：70-75

[14] Kleinrock L, Silvester J A. Optimum Transmission Radii for Packet Radio Networks or Why Six Is a Magic Number[A]//Proc. of Telecommunications Conf[C]. IEEE, 1978: 431-435

[15] Hou Ting-Chao, Victor L. Transmission Range Control in Multihop Packet Radio Networks[J]. IEEE Transactions on Communications, 1986, 34(1): 38-44

(上接第 104 页)

[5] Wallner D, Harder E, Agee R. Key Management for Multicast: Issues and Architecture [EB/OL]. [2008-4-20]. http://www.faqs.org/rfcs/rfc2627.html

[6] McGrew D A, Sherman A T. Key Establishement in Large Dynamic Groups using One-way Function Trees. IEEE Transactions on Software Engineering, 2003, 29(5): 444-458

[7] Kwak D, Lee S, Kim J, et al. An Efficient LKH Tree Balancing Algorithm for Group Key Management. IEEE Communications Letters, 2006, 10(3): 222-224

[8] Ng W H D, Howarth M, Sun Z I, et al. Dynamic Balanced Key Tree Management for Secure Multicast Communications. IEEE Transactions on Computers, 2007, 56(5): 590-605

[9] Eltoweissy M, Heydari H, Morales L, et al. Combinatorial optimization of group key management. Journal of Network and Systems Management, 2004, 12(1): 33-50