卫星组播多组共享密钥管理方案

孙雁鸣[1,2]，马恒太[1]，郑 刚[1]，易小伟[1,2]，潘 辉[1,2]
（1. 中国科学院软件研究所 天基综合信息系统重点实验室，北京 100190；
2. 中国科学院大学，北京 100190）

摘 要：现有的多组组密钥管理方案应用于大型动态卫星多组组播环境时，受卫星资源的限制，密钥管理效率成为瓶颈。设计了一种卫星多组组密钥管理方案SMGKM(Satellite Multiple Group Key Management)，根据对组播源的访问能力对用户进行分组，并在子组中设置子组管理者，通过构造组播密钥管理图和子组密钥管理结构进行多组组密钥管理，具有良好的前向和后向安全性，与现有典型方案相比，SMGKM有效降低了卫星的通信和存储开销，更适合大型动态卫星多组组密钥管理。

关键词：卫星组播；多组共享；组密钥管理；组密钥更新
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-1328(2013)06-0824-09
DOI：10.3873/j.issn.1000-1328.2013.06.012

Multiple Group Shared Key Management for Satellite Multicast

SUN Yan-ming[1,2], MA Heng-tai[1], ZHENG Gang[1], YI Xiao-wei[1,2], PAN Hui[1,2]
(1. Science and Technology on Integrated Information System Laboratory, Institute of Software Chinese Academy of Sciences, Beijing 100190, China;
2. University of Chinese Academy of Sciences, Beijing 100190, China)

Abstract: When existing group key management schemes are used in large and dynamic satellite multiple group key management, the efficiency is low due to the limitation of the satellite network. Key management is the bottleneck. To solve this problem, a new scheme named Satellite Multiple Group Key Management (SMGKM) is proposed in this paper. Users are divided into subgroups according to their access ability to the resources. Subgroup controllers are set in each subgroup. Multiple group key management is carried out by the construction of group key management graph and subgroup key management structure. The proposed scheme has forward and backward secrecy. In contrast with the existing schemes, SMGKM decreases the amount of keys stored in the satellite and the rekeying amount of the satellite efficiently. It is suited for multiple group key management under large and dynamic satellite multicast environment.

Key words: Satellite multicast; Multiple group sharing; Group key management; Group rekeying

0 引 言

卫星系统具有高带宽和优越的远程广播特性，能够支持大范围的组播新业务，借助卫星系统实现组播是组播技术的一个重要发展方向。在卫星组播应用中，需要对组播内容进行加密来保障其安全性。因此必须研究卫星组播通信中的组密钥管理问题，对组密钥进行高效分发和更新，确保卫星组播通信过程中密钥产生、传输、存储和使用的安全性。

目前，国内外对卫星组密钥管理的研究已取得了一些进展。文献[1]提出了分层的卫星组密钥管理协议。文献[2]针对LEO卫星环境提出了基于聚类的组密钥管理体系，有效降低对密钥更新的需求。文献[3]针对宽带卫星网络的特点，提出了基于LKH、分布式子群、辅助密钥延缓更新和成员自主计算相混合的层次型组密钥管理方案。文献[4]通过

收稿日期：2012-08-31； 修回日期：2012-12-14

构建分布式私钥生成中心,提出了基于身份的空间网络组密钥管理方案。文献[5]根据卫星网络特点,构造出分布式的组密钥管理方案,并给出组密钥更新消息的结构。文献[6]在前文的基础上,基于身份认证思想,结合双线性配对策略,给出更符合 LEO/MEO 空间结构的组密钥管理方法,密钥交换阶段仅需一轮通信。但上述组播通信研究并非针对多组组播通信而设计。在卫星组播应用中,会出现多组同时组播的情形,例如卫星同时转发多个电视节目,接收同一节目的用户构成一个组播组,用户可以根据需求加入其中某个组或者同时加入多个组。在该情形下,为保证通信的安全性需要解决卫星多组组播中的组密钥管理问题。

对多组组密钥管理问题的研究,国内外学者已提出了一些方案。文献[7]提出利用平衡密钥树进行层次性多组组密钥管理的方法。针对移动 Ad Hoc 网络,文献[8]提出了金字塔式的层次性多组组密钥管理方案,并进行了仿真实验。但是这两个方案[7-8]并不是针对一般情形设计的。对于多组组播来说,一般解决方案(General Key Management Scheme,GKMS)是按存在的组独立进行组密钥管理,当用户变动(加入/离开组)时,与用户变动相关的组都需要进行组密钥更新,以保证前向和后向安全性,因而组密钥管理的效率较低,可扩展性差。

文献[9]提出了采用多层共享集成密钥图进行组密钥管理的方案(Integration Graph Key Management,IGKM),平均效率高于 GKMS。但是,当用户在多组组播过程中进行用户变动时,IGKM 的效率会低于 GKMS。文献[10]提出了一种整合密钥树管理方案(Conformity Tree Key Management,CTKM),该方案减少了用户变动时的组密钥管理开销,平均效率高于 GKMS 和 IGKM。但当同时参加多个组播组的用户较少时,其效率会比 GKMS 更低。另外,文献[9-11]是针对地面组播应用设计的,并不适用于用户数目较多的动态卫星组播环境。

本文针对卫星多组组播环境,分析了不同应用场景下 GKMS、IGKM 和 CTKM 的优缺点,阐述了分层组密钥管理的设计思路,设计了卫星多组组密钥管理方案(Satellite Multiple Group Key Management,SMGKM),对上述几种方案的安全性和通信开销、计算开销、存储开销进行了对比分析。

1　卫星组播密钥管理分析

文中使用的符号及其说明见表 1 所示。

表 1　本文中所使用的符号

Table 1　Notation

符号	说明
n	组播组的数目
G	组集合
U	用户集合
u_i	卫星组播第 i 个用户
g_i	卫星组播第 i 个用户组
K	节点密钥
C_i	同类访问能力用户子组管理者

本文以单颗卫星的组播通信场景为例,为多组组播系统提供高效的组密钥管理,降低卫星组密钥更新代价。用户组集合 $G = \{g_1, g_2, \cdots, g_n\}$,用户集合 $U = \{u_1, u_2, \cdots, u_m\}$,$g_i \subseteq U(i = 1,2,\cdots,n)$。任意用户 u_i 可同时属于多个用户组。多组组密钥管理问题就在于如何对用户集合 U 进行分组生成组集合 G,使组成员变动时密钥管理的开销更小。

1.1　典型应用场景

本文针对 3 种典型应用场景来分析卫星组播多组组密钥管理需求。

场景 1. 在卫星电视广播应用中,卫星提供多个视频流组播。其中,每个视频流是一个组播源,组播源的授权用户可以收看相应的电视视频节目,各组播源独立进行数据加密保护。如果用户 u_i 要收看频道 1,那么需加入对应的用户组 g_1 来获得频道 1 的数据解密密钥。当 u_i 要收看频道 2 时,需先从 g_1 中退出,再加入 g_2,获得频道 2 的数据解密密钥。

该场景中,用户每次只能收看一个频道,不能同时加入多个组播组。由于各组播组之间相互独立,可采用 GKMS 进行组密钥管理。

场景 2. 在卫星视频会议应用中,用户组 g_1 和用户组 g_2 同时召开多方视频会议,卫星为视频会议提供组播服务。用户组中存在一类特殊用户 u_i,它需要同时加入 g_1 和 g_2。当这类特殊用户较多时,采用 GKMS 进行组密钥管理的效率很低。因为当特殊用户 u_i 退出或加入组通信时,为保证前向安全性和后向安全性,g_1 和 g_2 都需要进行组密钥更新,从而急

剧增加了组密钥更新开销。

场景3. 卫星电视广播应用中,卫星提供高清和一般质量两种视频信号。付费用户可接收高清信号,也可接收一般质量信号,免费用户只可接收一般质量信号。针对两类信号用两个组进行分别管理,g_1 管理接收一般质量视频信号的用户,g_2 管理接收高清质量视频信号的用户,免费用户只需加入 g_1,而付费用户需同时加入 g_1 和 g_2。如果存在较多付费用户时依然采用 GKMS 方案来管理密钥,那么付费用户退出组通信会引起较大的组密钥更新开销,严重影响组密钥管理效率。

对于场景2和场景3,IGKM 是可行的解决办法,该方案根据多组组播中用户访问能力的不同,对组中用户进行划分,将不同访问能力的用户划分在不同子树下,并由卫星集中管理。

1.2 现有密钥管理方案分析

IGKM 可适用于多组用户共享密钥管理,但存在如下问题。

首先,考虑用户访问能力切换的情形。如用户 u_i 从对 g_1 和 g_2 都具备访问能力切换到只对 g_1 具有访问能力。在该情形下,IGKM 具有比 GKMS 更低的效率。当用户 u_i 增加或减少对一个组的访问能力时,IGKM 在旧的子树删除此用户并在新的子树中添加该用户,需要更新两条密钥更新路径上的密钥。而 GKMS 只在一个组中添加或删除此用户,只需一条密钥更新路径上的密钥进行更新,总的密钥更新数量低于 IGKM。密钥更新路径是指在密钥树或密钥图中,从当前用户节点到所有可达的树根节点所经过节点所组成的路径。密钥更新路径上的节点就是进行密钥更新时需要变更的密钥集合。在实际应用中,对于多组通信的用户来说,这种只增加或减少一个组访问能力的情况可能经常发生。

其次,IGKM 并不适用于大型动态卫星多组组播环境。卫星对用户提供视频信号时,用户数量可能非常庞大。若采用 IGKM,除需保存所有用户的密钥,还需保存密钥图中所有中间节点的密钥,需要存储的密钥数量非常大。另外,为保证组通信的安全性,每当用户访问能力发生变化(加入某些组或离开某些组),卫星都要对密钥更新路径上的密钥进行更新,那么当大用户组频繁有用户加入或退出时,会由于密钥大量更新而导致用户组服务性能下降,影响正常服务能力。特别是当通过卫星进行组播时,由于卫星的存储空间和计算能力有限,影响会更大。当处于动态环境中时,用户经常变动,这种更新将造成巨大的通信开销。

CTKM[8] 在解决用户访问能力切换问题上与 IGKM 相比具有明显优势。CTKM 把所有用户合在一起构造一棵密钥树来管理。当用户访问能力切换时,只要该用户不离开组通信,就不需要对树结构进行更新,而只要用树结构来发送更新过的数据密钥,因而效率较高。但是 CTKM 也存在两个问题:第一,当用户零散地分布在各组中时,也就是说具有多个组访问能力的用户较少时,CTKM 效率会下降。这时采用 CTKM 等价于将多个组通信的组密钥管理集合在一起用一棵二叉密钥树来管理。此时采用 CTKM 的效率明显低于 GKMS。第二,CTKM 同样不适用于大型动态卫星多组组播。因为采用 CTKM 需要将所有组的用户集中在一起构造成一棵二叉树来管理。假设用户总数为 N,则卫星要存储 $2N-1$ 个密钥。当多组组播中的用户数量很大时,存储这些密钥将消耗大量的卫星资源,实际应用很难满足。另一方面,当加入或离开组通信的用户不断增加时,也会造成大量的通信开销,不但可能导致组通信信号延迟,甚至可能导致系统崩溃。

为解决以上问题,本文提出一种新的卫星多组组密钥管理方案 SMGKM。该方案适用于用户数量较多、访问能力经常发生变动的大型动态卫星组播环境,具有较高的密钥更新效率。

2 卫星多组组密钥管理方案设计

2.1 设计思路

按照对组播源的访问能力对用户进行分组。若存在 n 个组播源,即可得到 2^n-1 个访问能力子组。子组设置子组管理者,卫星仅对子组管理者进行管理。用户由子组管理者负责管理。当子组用户非常多时,子组管理者可能成为管理瓶颈,可在子组中对用户采取进一步组织管理。在实际应用中,只需对实际包含用户的子组进行管理。

组通信中通信内容先由数据密钥加密,再向用户组播。加密通信内容的数据密钥由卫星分发给子组管理者,然后由子组管理者分发给用户。卫星广

播时,用户可以用数据密钥解密得到通信内容。采用这种方案时,子组内的结构变化并不会对卫星造成影响。如当用户离开时,只要由用户所在子组的子组管理者发送消息通知卫星,然后卫星更新该用户所知的数据密钥就可以达到保证组通信安全的目的。通信中数据密钥数量远小于组管理结构中的用户密钥和密钥加密密钥。因此当用户频繁加入和离开子组时,由子组管理者对子组密钥更新来保证安全性。而组播管理层只需要更新少数的数据密钥就可以,总的密钥更新通信量远小于其它方案。

2.2　管理方案

2.2.1　管理流程

SMGKM 构造流程如图 1 所示。

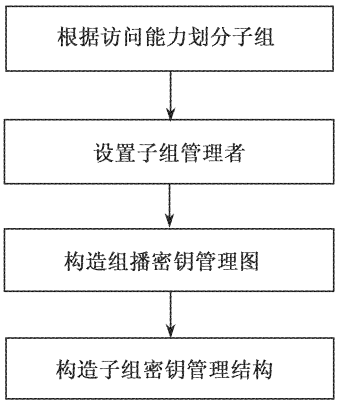

图 1　卫星多组组密钥管理方案构造流程

Fig. 1　Flow of SMGKM construction

(1) 根据访问能力划分子组,若存在 n 个组播源,则划分为 $2^n - 1$ 个访问能力子组。

(2) 设置子组管理者。对划分的子组进行编号,并分别设立子组管理者。将子组内所有用户按照其加入子组的次序建立一个队列,设置队首元素担任子组管理者,它负责本子组用户与卫星之间的密钥协商。有时,为提高子组内管理效率,可选具有较强计算和存储能力的用户担任子组管理者。

(3) 构造组播密钥管理图。组播源和所有子组管理者(子组的代表)采用密钥图的方式进行管理。组播源作为树根,具有访问能力的子组作为叶子,用二叉树结构将组播源与对它具有访问能力的子组连接起来,并合并相同部分形成组播密钥管理图。除管理密钥,组播密钥管理图还包括对组播内容进行加密的数据密钥。如图 2 所示,该场景中具有 3 个组播源与 7 个子组管理者。

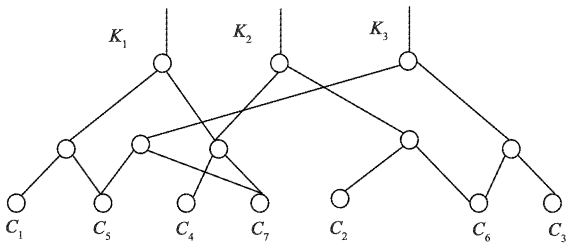

图 2　具有 3 个组播源的 SMGKM 组播密钥管理图

Fig. 2　SMGKM group key management graph for 3 resources

(4) 构造子组密钥管理结构。根据用户访问能力的不同,用户分别被划分到相应子组。由子组管理者对子组内用户进行管理。此时各子组间不存在相同用户。对子组用户较多的场景,可以采用进一步分层的结构,对子组用户进行管理。

2.2.2　密钥更新

当用户发生变动时,需要进行密钥更新来满足前向和后向安全性。SMGKM 密钥更新过程如下:

(1) 当新用户加入某子组时,由子组管理者更新子组密钥并通知卫星有新用户加入。卫星对该子组用户所拥有的数据密钥进行更新,然后用旧的数据密钥加密新的数据密钥,再组播给所有用户,拥有旧数据密钥的用户就可以解密得到新的数据密钥。然后再由新用户子组的子组管理者通知新用户新的数据密钥来完成密钥更新。当有用户离开时,由子组管理者更新子组密钥并通知卫星有用户离开,卫星对该子组用户拥有的数据密钥进行更新,将更新后的数据密钥用组播密钥管理图中的组密钥加密后组播给子组管理者,之后由子组管理者分发给用户。

(2) 当用户访问能力切换时,需要此用户通知新加入子组的子组管理者用户是由哪个子组切换而来,然后由新子组管理者通知卫星。卫星根据用户对组访问能力的增减,对相应的数据密钥进行更新。

(3) 当子组管理者主动离开子组时,它首先从子组用户中选出合适的新子组管理者,然后发送消息通知卫星。由新子组管理者与卫星通信协商建立个人密钥。卫星对组播密钥管理图进行更新,用新的子组管理者替代旧子组管理者的位置,并更新密钥图结构中旧子组管理者所拥有的密钥。子组内所有用户与新的子组管理者协商建立新的子组密钥。

组播密钥管理图更新步骤:用新子组管理者取代旧子组管理者;卫星与新子组管理者协商得个人

密钥 K;新子组管理者计算从当前节点到所有可达根节点之间的密钥,计算方法是从当前节点开始往上计算,设当前节点密钥为 K,其父节点的密钥就是 $f(K)$,其中 $f(\ )$ 为单向函数,若某节点有两个父节点,则左父节点密钥是 $f(\mathrm{ls}(K))$,右父节点的密钥是 $f(\mathrm{rs}(K))$($\mathrm{ls}(K)$ 表示将 K 左移一位,$\mathrm{rs}(K)$ 表示将 K 右移一位),一直计算到根节点;卫星将这些计算结果广播给其余用户。与传统组密钥更新相比,这种方法可以降低通信开销。

采用 SMGKM 进行多组的组密钥管理时,要求选择的子组管理者应能对其它子组内用户发送数据。对于只能接受而不能发送数据的用户在 SMGKM 中将受到限制,如某些传感器用户。当子组中有此类用户存在时,若存在可以对其它用户发送数据的用户,则在其中选择一个担当子组管理者;若子组内只存在只能接受数据的用户,就在组播密钥管理图设立一个虚拟的子组管理者,该子组内所有用户数据密钥的转发都直接由虚拟子组管理者负责,其实质是直接由卫星对该子组进行管理。

另外,当卫星发现某子组管理者为恶意节点时,会强行将其从组播密钥管理图中删除,子组会重建密钥管理结构。

SMGKM 组密钥更新流程如图 3 ~ 5 所示。

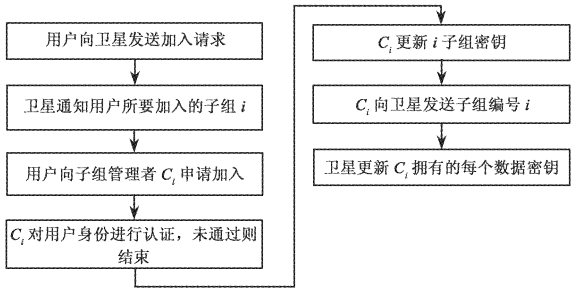

图 3 SMGKM 算法新用户加入密钥更新流程

Fig. 3 SMGKM rekeying flow when new user joins

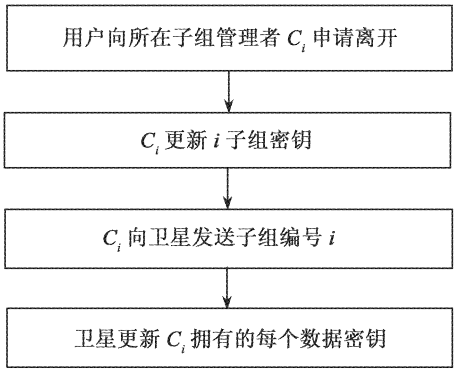

图 4 SMGKM 算法用户离开密钥更新流程

Fig. 4 SMGKM rekeying flow when user departs

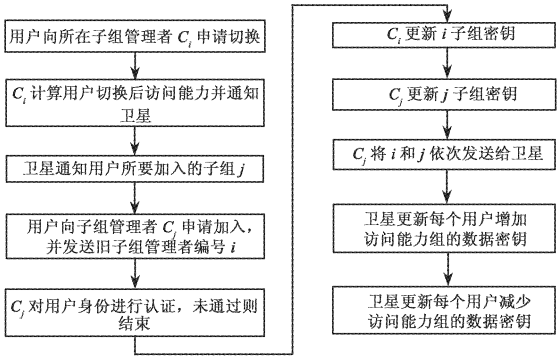

图 5 SMGKM 算法用户在子组间切换密钥更新流程

Fig. 5 SMGKM rekeying flow when user switches between subgroups

3 性能分析

3.1 安全性分析

本文提出的 SMGKM 方案具有保密性、前向和后向安全性和健壮性等特点。

首先,多组组通信中,各组的通信内容都先由数据密钥加密,组外用户无法获得数据解密密钥,因此无法解密通信内容,保证了组播数据的保密性。

其次,当有新用户加入时,根据用户具有的访问能力确定子组。用户所在子组的子组管理者需要向卫星发送消息通知卫星有新用户加入,而后卫星对这个子组拥有的数据密钥进行更新,从而使新用户得到更新后的数据密钥,而无法得到它加入之前的数据密钥,因此保证了后向安全性。

当有用户离开某组通信时,由用户所在子组的子组管理者通知卫星,卫星根据子组管理者的编号,对子组管理者拥有的数据密钥进行更新,子组的组密钥也进行更新,因此该用户曾拥有的密钥都得到了更新,它无法继续获得新的数据密钥,从而无法解密新的组通信内容,保障了前向安全性。

当用户在组间切换时,对于增加访问能力的组,相当于它作为新用户加入;对于减少访问能力的组,相当于它作为离开用户离开。SMGKM 中用户将原来所在子组的编号,通知它最后所在子组的子组管理者,并由子组管理者通知卫星。之后卫星对用户增加访问能力的组的数据密钥进行更新,保证了后向安全性;对用户减少访问能力的组的数据密钥进

行更新,保证了前向安全性。

最后,当卫星发现某子组管理者为恶意节点时,会强行将其从组播密钥管理图中删除,子组用户向卫星重新申请建立新子组管理者。因此,子组管理者即使被攻击,短时间内影响通信,也可很快得到恢复。另外,某子组被恶意影响,不会影响其它子组安全通信,因此 SMGKM 具有较好的健壮性。

3.2　效率分析

为了对 SMGKM 和 GKMS、IGKM、CTKM 进行性能比较,首先给出两个应用实例。

实例 1. 组集合 $G = \{g_1, g_2, g_3\}$,用户集合 $U = \{u_1, u_2, u_3, \cdots, u_{12}, u_{13}, u_{14}\}$。当用户加入组时,与各组之间关系如表 2 所示。

表 2　实例 1 中用户与组的关系

Table 2　Relation of users and group for case 1

用户/组	g_1	g_2	g_3
u_1, u_2	√		
u_3, u_4		√	
u_5, u_6			√
u_7, u_8	√	√	
u_9, u_{10}	√		√
u_{11}, u_{12}		√	√
u_{13}, u_{14}	√	√	√

实例 2. 组集合 $G = \{g_1, g_2, g_3\}$,用户集合 $U = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7\}$。用户与组间关系如表 3 所示。该实例中只有 u_7 具有对多个组访问的能力,其它用户都只能访问 1 个组。

表 3　实例 2 中用户与组的关系

Table 3　Relation of users and group for case 2

用户/组	g_1	g_2	g_3
u_1, u_2	√		
u_3, u_4		√	
u_5, u_6			√
u_7	√	√	√

假设采用二叉树结构进行组密钥管理。当有用户加入时,用单向函数计算中间节点的更新密钥,然后将新的中间节点密钥通知给新加入用户。当有用户被删除时,用当前用户节点的兄弟节点替代其父节点。数据组播前需要用数据密钥对组播内容加密,因此密钥更新时除树结构中的密钥外,还需要更新数据密钥。与用户数量相比,SMGKM 的子组管理者数量很少,因此假定子组管理者不发生变动。下面分别从卫星所需更新密钥数 R、密钥分发次数 T、卫星所需存储密钥数 S 来考察 GKMS、IGKM、CTKM、SMGKM 的密钥管理开销。

(1) 当有用户退出组通信时

通常情况下,如果多组通信中同时存在 n 个组,采用 GKMS 时需要建立 n 棵密钥树独立进行管理。为简单起见,假定密钥树是满二叉树。当有用户 u_k 离开组通信时,卫星所需密钥管理开销为:

$$R = \sum_{i=1}^{m} \log_2 N_i \tag{1}$$

$$T = \sum_{i=1}^{m} [2(\log_2 N_i - 1) + 1] = \sum_{i=1}^{m} (2\log_2 N_i - 1) \tag{2}$$

$$S = \sum_{i=1}^{n} (2N_i - 1 + 1) - 2m = 2\sum_{i=1}^{m} N_i - 2m \tag{3}$$

其中 m 表示用户 u_k 所在组的个数,N_i 表示各组中用户的数量。

采用 IGKM 进行管理,当 u_k 离开组时,卫星密钥管理开销与整合密钥图的构造方式以及用户的访问能力分布有关。文献[4]采用了合并子树的方法,所需存储密钥数 S 的上限为未合并前的整合密钥图中密钥总数。

采用 CTKM 管理时卫星所需密钥管理开销为:

$$R = \log_2 N + m - 1 \tag{4}$$

$$T = 2(\log_2 N - 1) + m = 2\log_2 N + m - 2 \tag{5}$$

$$S = 2N - 1 - 2 + n = 2N + n - 3 \tag{6}$$

其中 N 为用户总数,m 为 u_k 可访问组的个数。

采用 SMGKM 进行管理时,当 u_k 离开组通信,卫星需要更新的密钥数 R 和密钥分发次数 T 都为 m。m 表示 u_k 具有访问能力的组的个数。卫星所需存储密钥数 S 与多组通信中同时存在的组个数以及组播管理层构造方式有关,远小于组通信中的用户数。另外,SMGKM 不只能减少卫星更新的密钥数,其星地更新密钥总和也低于 IGKM。

对于实例 1,当 u_7 退出组通信时,各方案性能比较如表 4 所示。可以看出,GKMS 的卫星密钥管理开销最多,CTKM 与 IGKM 相似,SMGKM 最少。

(2) 用户只增减一个组的访问能力

通常情况下,如果组通信中同时存在 n 个组,对用户采用 IGKM 进行管理,当一个用户访问能力切换时,总的种类数(不包含加入和离开) W 为:

表4 场景1中 u_7 退出组通信时的比较

Table 4 Comparison when user u_7 departs from group communication for case 1

方案\性能指标	R	T	S
GKMS	6	10	44
IGKM	5	8	30
CTKM	5	8	28
SMGKM	2	2	18

$$W = (2^n - 1)(2^n - 1) - (2^n - 1) = (2^n - 1)(2^n - 2)$$

只增减一个组访问能力的切换种类数 W_1 为：

$$W_1 = 2[C_n^1(n-1) + C_n^2(n-2) + \cdots + C_n^{n-1}] = 2^n n - 2n = 2n(2^{n-1} - 1)$$

$$W_1 : W = \frac{2^n n - 2n}{(2^n - 1)(2^n - 2)} = \frac{n}{2^n - 1} \tag{7}$$

实例1中，u_7 从对组1、组2具有访问能力切换到只对组1具有访问能力时(即退出组2)，各方案比较如表5所示。可以看出，该情况下，IGKM更新密钥数和密钥分发次数高于其它方案。SMGKM卫星密钥管理开销最少。因为当用户增减一个组访问能力时，IGKM需要更新两条密钥路径。

表5 场景1中 u_7 退出组2时的比较

Table 5 Comparison when user u_7 departs from group 2 for case 1

方案\性能指标	R	T	S
GKMS	3	5	46
IGKM	6	9	32
CTKM	1	3	30
SMGKM	1	1	18

(3) 对多个组具有访问能力的用户较少时

与GKMS相比，对多个组具有访问能力的用户越少，CTKM效率越低。假设存在 n 个组，用户总数为 N，每个用户只加入一个组。用户在各组平均分布，每组用户数为 N/n。当有一个用户离开时，采用GKMS，更新密钥数为 $\log_2(N/n)$，密钥分发次数为 $2\log_2(N/n) - 1$，而采用CTKM，更新密钥数为 $\log_2 N$，密钥分发次数为 $2\log_2 N - 1$。在此情形下，采用CTKM需要更新密钥数和密钥分发次数都比GKMS多。

实例2中只有用户 u_7 具有多个组的访问能力，u_1 离开组通信时，各方案比较如表6所示。可以看出，若对多个组具有访问能力的用户较少，当用户离开组通信时，CTKM方案的更新密钥数与密钥分发次数高于其他方案。

表6 场景2中 u_1 离开组通信时的比较

Table 6 Comparison when user u_1 departs from group communication for case 2

方案\性能指标	R	T	S
GKMS	2	3	16
IGKM	2	3	14
CTKM	3	5	14
SMGKM	1	1	10

(4) 建立子组密钥管理结构开销分析

初始构建阶段需要根据存在的访问能力子组构造组播密钥管理图。若某子组无用户，则不需在图中设立位置。卫星主要开销包括保存各子组用户队列的存储开销和把密钥分发给子组管理者的通信开销。分发密钥的通信开销与通信数据源数、子组数以及组播密钥管理图的构造方式有关。如图2结构中，除卫星与子组管理者协商的个人密钥外，卫星需要分发的密钥次数为19，其中包括组播管理图中所有辅助密钥以及数据密钥。

当多组通信中包含 n 个组播源时，组播密钥管理图构建阶段的密钥分发次数 T 满足：

$$T \leqslant 2^n n - n \tag{8}$$

另外，各子组需要构建子组密钥管理结构，该开销与子组用户数量有关。除组内用户需要与子组管理者协商个人密钥外，还需分发管理结构中的辅助密钥和子组密钥。为讨论方便，假定子组中只存在一个集中管理中心(实际应用中可能采用分层的子组管理结构)，假定子组管理结构为满二叉树。此时子组管理者所需密钥分发次数 T_i 为：

$$T_i = 2N_i - 2 \tag{9}$$

其中 N_i 为该子组内用户总数。

子组管理者需要保存子组管理结构中所有节点的密钥，因而子组管理者的存储开销 S_i 为：

$$S_i = 2N_i - 1 \tag{10}$$

其中 N_i 为该子组内用户总数。

另外，子组管理者作为组播密钥管理图的成员，还需要保存个人密钥，以及组播管理图中的辅助密钥和数据密钥。所需存储密钥数与组播源数及组播管理层构造方式有关。

4　仿　真

在具有高误码、大时延的卫星网络中,通信开销成为影响系统性能的关键。仿真中,卫星为密钥管理中心,主要考察各方案进行组密钥更新时星地通信的带宽开销,加密算法采用椭圆曲线算法,密钥长度设定为 160 比特,网络带宽为 20Mbps,仿真工具采用 Matlab 7.0,测试采用 3 个组播源。

(1) 用户在各访问能力子组服从均匀分布。用户总数设为 7×2^{11} 个,SMGKM 根据对组的访问能力划分为 7 个子组,各子组用户数相同。用户请求分三类:加入组、离开组和访问能力切换,共测试 1000 次随机请求。在此,访问能力切换只测试从对某组有访问能力切换到除此组外对其它组有访问能力。

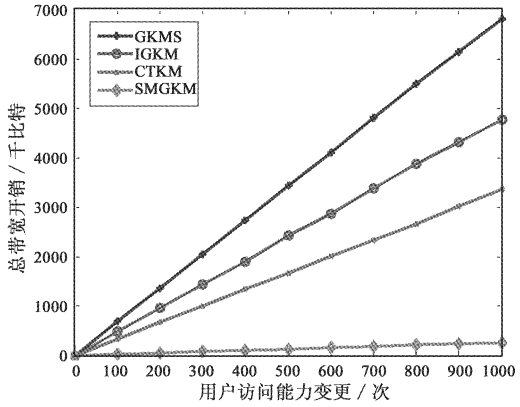

图 6　用户访问能力变更时的带宽开销

Fig. 6　Bandwidth consumption when user changes access capability

仿真结果表明,此时 SMGKM 组密钥更新总带宽开销是 GKMS 的 5%,是 IGKM 的 7%,是 CTKM 的 10.1%。

(2) 用户只增减一个组的访问能力。用户总数设为 7×2^{11},SMGKM 根据对组的访问能力划分为 7 个子组,各子组用户数相同。只测试用户切换请求,且切换只增减一个组的访问能力。这类切换共有 18 种,进行 1000 次切换操作,每种切换发生的可能占 1/18,测试结果如图 7 所示。

仿真结果表明,此时 IGKM 组密钥更新带宽开销最高,而 CTKM 优于 GKMS 和 IGKM。此时 SMGKM 组密钥更新总带宽开销最低,是 GKMS 的 4.9%,是 IGKM 的 2.6%,是 CTKM 的 12.7%。

(3) 当具有多个组访问能力的用户较少时。用户总数设为 3×2^{11},每个用户仅加入一个组。SMGKM 根据访问能力划分为 7 个子组,其中 3 个子组用户数为 2^{11},另外 4 个子组用户数为 0。所有用户随机发生加入或离开请求,共测试 1000 次,测试结果如图 8 所示。

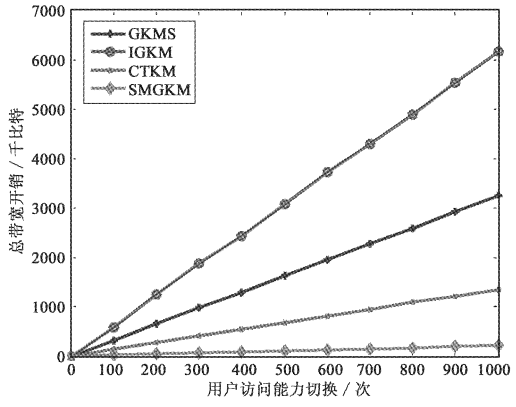

图 7　用户访问能力切换带宽开销

Fig. 7　Bandwidth consumption when user switches access capability

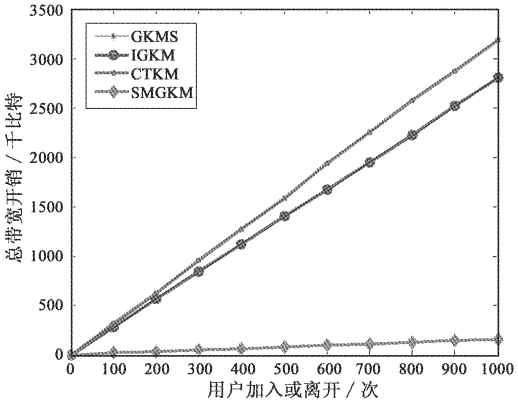

图 8　用户访问能力零散时的带宽开销

Fig. 8　Bandwidth consumption when users access capability are scattered

仿真结果表明,此时 CTKM 组密钥更新带宽开销略高于其它方案,这是因为 CTKM 需要将所有用户构造成一棵密钥树。IGKM 与 GKMS 带宽开销相同。此时 SMGKM 组密钥更新总带宽开销是 GKMS 的 5.7%,是 IGKM 的 5.7%,是 CTKM 的 4.8%。

5　结　论

本文研究了卫星组播通信环境下的多组组密钥管理问题。针对不同场景分析了现有组播密钥管理方案的优缺点,提出了一种卫星多组组密钥管理方

案SMGKM,该方案具有良好的前向和后向安全性,通过将卫星多组组密钥管理的存储和通信开销分散到各子组管理者中,有效降低了卫星组密钥更新时的带宽和存储开销。仿真结果表明,与GKMS、IGKM和CTKM相比,SMGKM更适合大型动态卫星多组组密钥管理。

参 考 文 献

[1] Yavuz A A, Alagz F, Anarim E. NAMEPS: n-tier satellite multicast security protocol based on signcryption schemes[C]. IEEE Global Telecommunications Conference, San Francisco, USA, November 27 - December 1, 2006.

[2] Hubenko V P, Raines R A, Baldwin R O, et al. Improving satellite multicast security scalability by reducing rekeying requirements[J]. IEEE Network, 2007, 21(4): 51 - 56.

[3] 李伟娜, 郑康锋, 杨义先. 宽带卫星网络组播密钥管理方案研究[C]. 第十三届全国青年通信学术会议,山东,中国, 2008年11月1 - 2日.[Li Wei-na, Zheng Kang-feng, Yang Yi-xian. Research on multicast key management scheme for broadband satellite network [C]. The 13th National Youth Conference on Communication, Shandong, China, November 1 - 2,2008.]

[4] 罗长远, 李伟, 霍士伟. 基于身份的空间网络组密钥管理方案[J]. 通信学报, 2010, 31(12):104 - 110.[Luo Chang-yuan, Li Wei, Huo Shi-wei. Identity-based group key management scheme for space networks [J]. Journal on Communications, 2010, 31(12): 104 - 110.]

[5] 王宇, 卢均, 吴忠望. 空间信息网络的组密钥管理[J]. 宇航学报, 2006, 27(3):533 - 555.[Wang Yu, Lu Jun, Wu Zhong-wang. Multicast key management of space information network[J]. Journal of Astronautics, 2006, 27(3): 553 - 555.]

[6] 钟焰涛, 马建峰. LEO/MEO双层空间信息网中基于身份的群组密钥管理方案[J]. 宇航学报, 2011, 32(7):1551 - 1556.[Zhong Yan-tao, Ma Jian-feng. Identity based group key management scheme for LEO/MEO double-Layer space information network[J]. Journal of Astronautics, 2011, 32(7): 1551 - 1556.]

[7] Ng W H D, Sun Z L. Multi-layers balanced LKH[C]. IEEE International Conference on Communications, Seoul, Korea, May 16 - 20, 2005.

[8] Bo R, Chen H H, Qian Y, et al. A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: the key management study[J]. IEEE Transactions On Vehicular Technology, 2009, 58(1): 398 - 408.

[9] Sun Y, Liu K J R. Hierarchical group access control for secure multicast communications [J]. IEEE/ACM Transactions On Networking, 2007, 15(6): 1514 - 1526.

[10] 李晓东. 一种多组共享的高效组密钥管理方案[J]. 北京电子科技学院学报,2008,16(4):19 - 24.[Li Xiao-dong. An effective multiple group sharing group key management solution [J]. Journal of Beijing Electronic Science and Technology Institute, 2008, 16(4): 19 - 24.]

[11] Aparna R, Amberker B B. Key management scheme for multiple simultaneous secure group communication [C]. IEEE International Conference on Internet Multimedia Services Architecture and Applications, Bangalore, India, December 9 - 11, 2009.

作者简介:

孙雁鸣(1978 -),男,博士研究生,主要研究方向为卫星组网通信与信息安全。

通信地址:北京市海淀区中关村南四街4号中国科学院软件研究所天基综合信息系统重点实验室(100190)

电话:15011337216

E-mail:953740301@qq.com

(编辑:余 未)