LEO/MEO 双层空间信息网中基于身份的群组密钥管理方案

钟焰涛，马建峰
（西安电子科技大学计算机网络与信息安全教育部重点实验室，西安 710071）

摘 要：由于空间信息网中结点的移动性，在空间信息网中实现传统的群组密钥管理面临许多困难。根据空间信息网的特点，分析了空间信息网中群组密钥管理方案的需求，设计了一个适用于 LEO/MEO 双层空间信息网络的群组密钥管理方案，采用基于身份的思想，消除了对证书系统的依赖，能在空间信息网中灵活高效地实现。将空间信息网中的结点根据其逻辑位置划分为簇，其中簇头为 MEO 卫星，在密钥交换阶段中共享密钥仅由所有簇头结点决定，这种机制大大减少了通信量。方案能有效抵抗外部攻击者，并且具有前向保密性和后向保密性。仿真实验表明，方案具有很高的通信效率。

关键词：空间信息网；LEO/MEO 双层结构；群组密钥管理；认证
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-1328(2011)07-1551-06
DOI：10.3873/j.issn.1000-1328.2011.07.017

Identity Based Group Key Management Scheme for LEO/MEO Double-Layer Space Information Network

ZHONG Yan-tao, MA Jian-feng
(The Ministry of Education Key Laboratory of Computer Networks and Information Security , Xidian University, Xi'an 710071, China)

Abstract: Many studies are conducted on security for space information networks composed of a small number of ground stations and relatively more satellites - about several dozens in normal condition. A group key management is used to implement secure communication in space information networks in this paper. It is difficult to implement the traditional group key management scheme in a space information network due to its dynamic topology. Based on the analysis of features of LEO/MEO double-layer space information network, a novel identity based group key management scheme is proposed in which all nodes in a space information network are divided into clusters and MEO satellites are used as cluster heads. Further more, in group key establishment step, only cluster heads are devoted into the group key. Thus traffic of our scheme is greatly reduced. Additionally, security analysis shows that the proposed scheme achieves both forward security and backward security, and security against outside attackers. Simulations show that the proposed scheme takes advantage of high communication efficiency.

Key words: Space information network; LEO/MEO double-layer structure; Group key management; Authentication

0 引 言

空间信息网(Space Information Network, SIN)是一个天、空、地一体化的网络系统，由在空间中具有通信能力的各种通信卫星、资源卫星和地面控制结点组成。空间信息网的骨干通信网是由在轨运行的卫星组成的卫星星座系统。空间信息网具有覆盖面广、组网方式灵活、不受地理环境限制等特点，能

收稿日期：2010-07-23； 修回日期：2010-11-16
基金项目：国家自然科学基金(60872041, 60573036, 60702059, 60503012)；国家自然科学基金重点项目(60633020)

够为许多紧急任务以及科研任务如气象观察、环境与灾害监测、资源勘察、科学探测提供通信服务，成为新型网络研究的新方向[1]。

如图1所示，由低地球轨道(Low Earth Orbit, LEO)卫星和中地球轨道(Medium Earth Orbit, MEO)卫星组成的双层空间信息网络具有强容错性、无缝覆盖等优点。相对于单层结构，LEO/MEO双层结构可以利用MEO卫星进行网络管理，能有效提高网络资源利用率，简化空间信息网的结构，LEO卫星星座则可以充当接入网络。具有LEO/MEO双层结构的空间信息网逐渐成为研究热点[2]。

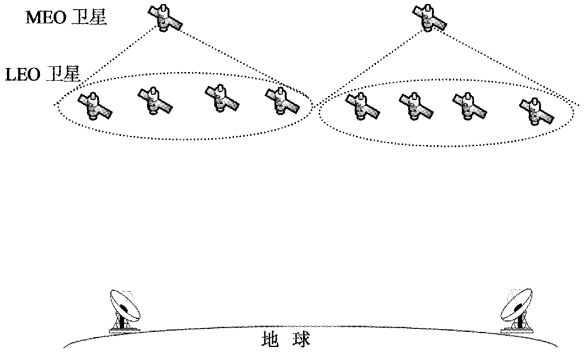

图1 LEO/MEO双层结构的空间信息网

Fig. 1 MEO/LEO double-layer space information network

由于空间信息网结点之间的通信具有开放性，空间信息网中传输的数据很容易被非授权者甚至恶意攻击者截获从而引发大量安全性问题。在通信系统中，使用群组密钥对通信进行加密是一个能够保证多个结点之间安全通信的普遍而有效的方法。为保证空间信息网的通信安全，在空间信息网内实现群组密钥管理成为一个重要课题。

国内外学者已经提出了许多安全高效的方案实现传统网络中的群组密钥管理[3-4]。然而，空间信息网中结点的高速运动、动态拓扑等突出特点使得原有群组密钥管理方案难以在空间信息网中得以有效应用，同时原有群组密钥管理方案也没有利用空间信息网中结点运动周期性和卫星结点分层等特征，不能有效提高方案在空间信息网中的运行效率。文献[5]提出了一个空间信息网中的群组密钥交换协议，能在保证密钥传播效率的同时，提高密钥系统的可靠性。该协议基于公钥基础设施，但并未指出公钥基础设施如何配置，同时该协议未给出安全性证明。

本文根据空间信息网的通信特点，设计了一个适用于LEO/MEO双层空间信息网络的简单、高效率且安全的群组密钥管理方案，该方案采用基于身份的思想，基于身份的系统消除了对证书的依赖，可以在空间信息网中灵活高效地实现。安全性分析表明该方案不仅能有效抵抗外部攻击者，还具有前向保密性和后向保密性。仿真结果表明，该方案具有密钥建立速度快且通信量小的优点，通信效率很高。

1 基于身份的密码系统

1984年Shamir试图绕开基于目录的公钥基础设施的束缚，提出了基于身份密码系统(Identity Based Cryptosystem, IBC)的思想[6]。在IBC中，用户的公钥就是用户的身份信息，因此很自然地解决了公钥与实体身份的绑定问题，而用户的私钥由可信的密钥生成中心(Key Generate Center, KGC)根据用户公钥和系统的主密钥生成。目前IBC已经相当成熟，成为了继基于证书中心(Certificate Authority, CA)密码学之后的公钥密码体制中的另外一个重要发展方向，并且在多个领域得到广泛应用[7]。

2 空间信息网中群组密钥管理的安全需求和性能需求

空间信息网中群组密钥管理方案的主要安全需求和性能需求包括：

(1) 认证性。认证性要求外部攻击者即使能够监听所有的网络流量并试图仿冒群组内部成员，能够计算出群组密钥的概率也是可忽略的。认证性保证了仅有群组内部成员可以计算出群组密钥，从而保证了密钥安全性。

(2) 前向保密性。当新结点加入群组或者当前密钥泄漏时，前向保密性能够保证过去使用的密钥的安全性。

(3) 后向保密性。当结点退出群组或者已使用的密钥泄漏时，后向保密性能保证将来使用密钥的安全性。

(4) 通信效率高。空间信息网中卫星结点之间距离远，通信时延长、误码率高，需要通信效率高，通信轮数少的方案。

3　方案构造

3.1　基本思想

系统中的密钥生成中心 KGC 设为卫星地面站。地面站具有很高的计算能力和抗攻击能力,能够保证系统主密钥和用户私钥的安全性。

空间信息网中的群组成员根据其所在逻辑位置划分为不同的簇[8],其中簇头结点为 MEO 卫星,簇内成员包括簇头 MEO 卫星所能覆盖的所有 LEO 卫星。当一颗 LEO 卫星移动到一个新的簇内时,需要向簇头 MEO 卫星注册。注册阶段完成后,所有的簇头结点之间进行群组密钥交换操作建立一个共享密钥;之后每个簇头结点通过加入盲因子方式秘密地将共享密钥发送给各簇内的 LEO 卫星结点。和分布式的群组密钥协商相比,这种仅由簇头结点协商建立共享密钥的机制无需 LEO 卫星参与密钥的生成,大大减少了通信量,同时因为所有簇内结点均在簇头结点的覆盖范围内,所以簇头结点向簇内结点发送密钥仅需簇头的一次广播就可以实现。

在有结点加入群组或退出群组时,为了保证密钥的前向保密性和后向保密性,需要对群组密钥进行更新。密钥更新时,所在簇内成员发生变动的簇的簇头结点向其它簇头结点发送一个新的随机值,所有簇头结点根据该随机值更新共享密钥并广播给簇内的 LEO 卫星结点。

3.2　系统初始

在系统初始阶段,KGC 选取系统参数并为空间信息网中所有结点生成私钥。

KGC 选取大素数 q,两个 q 阶群 G_1、G_2,以及双线性映射 e: $G_1 \times G_1 \to G_2$。选取随机值 $s \in Z_q^*$,并计算 $P_{\text{pub}} = sP$,其中 P 是 G_1 群的生成元。选取安全的密码学哈希函数 H_1: $\{0,1\}^* \to Z_q^*$ 和 H_2: $G_2 \to Z_q^*$。然后公开$\langle q, G_1, G_2, e, P, P_{\text{pub}}, H_1, H_2\rangle$为系统公开参数。

身份标识为 ID 的结点公钥为 $q_{\text{ID}} = H_1(\text{ID})$,KGC 为该结点生成私钥 $s_{\text{ID}} = (s + q_{\text{ID}})^{-1}P$。

3.3　注册阶段

当一颗 LEO 卫星结点切换到一个簇头 MEO 卫星的覆盖范围时必须向该簇头结点注册。身份标识为 L 的 LEO 卫星具有私钥 $s_L = (s + q_L)^{-1}P$,向身份标识为 M 的 MEO 卫星注册过程如下。L 选取秘密随机值 $r \in Z_q^*$,计算 rP,$r(s + q_L)^{-1}P$,并发送$\langle L, rP, r(s + q_L)^{-1}P\rangle$给 M;M 验证等式 $e(P_{\text{pub}} + q_L P, r(s + q_L)^{-1}P) = e(P, rP)$ 成立后,记录$\langle L, rP\rangle$并发送注册成功信息给 L,同时将 L 记录为簇内结点。

3.4　密钥交换

群组密钥需要定期更换,以减少密钥泄漏带来安全性威胁,因此密钥交换阶段必须定期执行。执行周期可以事先设定,也可以根据密钥使用频率适应性地调整。使用频率较高的密钥泄漏的可能性较大,应缩短其使用期限。

本文方案的密钥交换阶段仅需一轮通信。假设共有 n 个 MEO 卫星结点参与密钥交换,分别记为 $M_1, M_2, \cdots, M_n$。对于 $1 \leqslant i \leqslant n$,每个 M_i 均执行以下两步:

(1) 通信阶段:选取随机值 $a_i \in Z_q^*$,对于 $1 \leqslant j \leqslant n$ 且 $i \neq j$,计算 $T_{i,j} = a_i(P_{\text{pub}} + q_{M_j}P)$,广播$\langle T_{i,1}, T_{i,2}, \cdots, T_{i,i-1}, T_{i,i+1}, \cdots, T_{i,n}\rangle$给所有的 MEO 卫星。

(2) 计算阶段:对于 $1 \leqslant j \leqslant n$ 且 $i \neq j$,M_i 收到所有的 $T_{j,i}$ 后计算中间值

$$\begin{aligned} T &= e(T_{1,i} + T_{2,i} + \cdots + T_{i-1,i} + a_i(P_{\text{pub}} + q_{M_i}P) + T_{i+1,i} + \cdots + T_{n,i}, s_{M_i}) \\ &= e((a_1 + a_2 + \cdots + a_n) \cdot (s + q_{M_i})P, (s + q_{M_i})^{-1}P) \\ &= e(P,P)^{a_1 + a_2 + \cdots + a_n} \end{aligned}$$

并计算群组密钥为

$$K = e(H_2(T)P, P) = e(P,P)^{H_2(T)}$$

3.5　密钥分发

计算出群组密钥以后,簇头 MEO 卫星要将群组密钥秘密地分发给簇内 LEO 卫星。身份标识为 M 的 MEO 卫星向身份标识为 L 的 LEO 卫星分发密钥的过程如下:

(1) 计算 $T^* = H_2(T)(rP)$,并发送给 L;

(2) L 计算群组密钥为

$$\begin{aligned} K &= e(T^*, r^{-1}P) \\ &= e(H_2(T) \cdot rP, r^{-1}P) \\ &= e(P,P)^{H_2(T)} \end{aligned}$$

3.6　结点加入

由于每个簇头结点均保存了当前群组中所有 LEO 卫星结点的记录,一旦某个簇头 M_i 结点发现有新的 LEO 卫星结点注册,该簇头结点选取随机值

$a^* \in Z_q^*$，计算 $T'_{i,j} = a^*(P_{pub} + q_{M_j}P)(1 \leqslant j \leqslant n$，且 $i \neq j)$，广播$\langle T'_{i,1}, T'_{i,2}, \cdots, T'_{i,i-1}, T'_{i,i+1} \cdots, T'_{i,n}\rangle$ 给所有的 MEO 卫星。簇头结点 M_j 收到 $T'_{i,j}$ 后计算

$$T = T_0 \cdot e(T'_{i,j}, s_{M_j})$$
$$= T_0 \cdot e(P,P)^{a^*}$$

其中，T_0 为上次计算密钥过程的中间值 T，更新群组密钥为

$$K = e(H_2(T)P,P) = e(P,P)^{H_2(T)}$$

然后使用 3.5 节的步骤分发密钥。

3.7 结点退出

当一个 LEO 结点向簇头结点提出退出群组或被簇头结点删除出群组时，为了保证群组密钥的后向安全性，密钥也需要进行更新。更新过程和 3.6 节所述由结点加入引起的密钥更新过程相同。

4 安全性分析

在安全性分析中，攻击者可以搜集到所有的系统公开参数和密钥管理方案执行中的所有通信消息，这反映了空间信息网中的通信是开放的、易被攻击者截获的。同时，允许攻击者向空间信息网中的卫星结点发送消息，这反映了攻击者有可能试图仿冒网络中某一颗或多颗卫星参与协议。

方案的安全性分析由以下两条引理及三条定理给出，分析结果表明方案满足认证性、前向保密性和后向保密性。

引理 1. 攻击者在注册阶段中仿冒 LEO 卫星向簇头 MEO 卫星注册成功的概率可忽略。

证. 假设攻击者以不可忽略的概率 ε 成功地在注册阶段中仿冒某 LEO 卫星向簇头 MEO 卫星注册。令该 LEO 卫星的身份标识为 L。根据注册阶段的描述，若攻击者注册成功，攻击者必然向簇头 MEO 卫星发送注册请求$\langle L, P_1, P_2\rangle$，其中 P_1 和 P_2 满足 $e((s+q_L)P, P_2) = e(P, P_1)$，即，满足 $e(P, P_2) = e((s+q_L)^{-1}P, P_1)$。进一步，对于 G_1 群上的任一值 P'，攻击者能够通过验证 $e(P, P_2) = e(P', P_1)$ 是否成立确定 P' 等于$(s+q_L)^{-1}P$。

攻击者可以从系统公开参数中计算出 $(s+q_L)P = P_{pub} + q_L P$，但不知道 L 的私钥$(s+q_L)^{-1}P$，这意味着攻击者能够以 ε 的概率判断 G_1 群上的随机值是否等于$(s+q_L)^{-1}P$，这与整除判定性 Diffie-Hellman（Divisible Decisional Diffie-Hellman，DDDH）假设[9]相矛盾，故引理得证。

引理 2. 攻击者仿冒 MEO 卫星参与密钥交换后能计算出群组密钥的概率可忽略。

证. 假设攻击者在仿冒 MEO 卫星参与密钥交换后，能以不可忽略的概率 ε 成功地计算出群组密钥。令攻击者仿冒的 MEO 卫星为 M_i。根据密钥交换阶段的描述，当攻击者计算出群组密钥时，攻击者必然先计算出

$$T = e(P,P)^{a_1+a_2+\cdots+a_n}$$

其中 a_1，a_2，…，a_n 分别是参与密钥交换的各 MEO 卫星选定的随机值。进一步地，对于 G_1 群上的任意值 P''，攻击者能够通过验证 $T = e(P, P'')$ 是否成立确定 P'' 等于$(a_1 + a_2 + \cdots + a_n)P$。攻击者不知道 M_i 的私钥$(s+q_{M_i})^{-1}P$，但是可以从系统公开参数及密钥交换的通信阶段收集的信息计算出

$$(a_1 + a_2 + \cdots + a_n) \cdot (s + q_{M_i})P$$
$$= T_{1,i} + T_{2,i} + \cdots + T_{i-1,i} +$$
$$a_i(P_{pub} + q_{M_i}P) + T_{i+1,i} + \cdots + T_{n,i}$$

以及 $(s+q_{M_i})P = P_{pub} + q_{M_i}P$。这意味着攻击者在知道$(a_1 + a_2 + \cdots + a_n) \cdot (s + q_{M_i})P$ 和$(s+q_{M_i})P$ 的情况下，能够以 ε 的概率判定 G_1 群上的随机值是否等于$(a_1 + a_2 + \cdots + a_n)P$，这与 DDDH 假设[9]相矛盾，故引理得证。

定理 1. 群组密钥管理方案是认证安全的。

证. 对认证性的攻击分为被动攻击和主动攻击。被动攻击者收集系统公开参数和各阶段中卫星结点间的消息通信，试图计算出群组密钥。主动攻击的途径有两条：其一，在注册阶段冒充合法 LEO 卫星结点向 MEO 簇头注册，注册成功后能够在密钥分发阶段计算出群组密钥；其二，冒充某些 MEO 结点参与密钥交换，试图在密钥交换后计算出群组密钥。

（1）首先考虑被动攻击。被动攻击者仅有两种可能计算出密钥的方法：要么通过在密钥交换中收集的信息计算出中间值 T，进一步计算出 $H_2(T)$ 和密钥 K；要么通过在注册阶段和密钥分发阶段收集的信息计算出群组密钥 K。由于 H_2 是安全的密码学哈希函数，所以攻击者在注册阶段和密钥分发阶段收集的信息无助于攻击者计算 T 的值，同时攻击者在密钥交换阶段收集的信息无助于攻击者不通过中间值 T 计算 K。

在密钥交换阶段,被动攻击者的攻击能力不大于引理 2 中所述攻击者的攻击能力。由引理 2 可知,被动攻击者通过密钥交换阶段收集的通信消息能够计算出 T,进而计算出密钥 K 的概率可忽略。

假定攻击者能够以不可忽略的概率 ε 成功地通过在注册阶段和密钥分发阶段收集的信息计算出群组密钥 K。当攻击者计算 K 成功时,假设任一 LEO 卫星 L 在注册阶段选定的秘密随机值为 r,对于 G_1 群上的任意值 P''',攻击者可以通过验证 $e(T^*, P''') = K$ 是否成立确定 $P''' = r^{-1}P$ 是否成立。即攻击者在知道 $T^* = H_2(T)(rP)$ 和 rP 的情况下,能够以 ε 的概率判定 G_1 群上的随机值是否等于 $H_2(T)P$, 这与 DDDH 假设[9]相矛盾。

(2) 其次考虑主动攻击。由引理 1 可知,攻击者在注册阶段中仿冒任一 LEO 卫星向簇头 MEO 卫星注册成功的概率可忽略;由引理 2 可知,即使攻击者能够仿冒 MEO 卫星参与密钥交换,攻击者能计算出群组密钥的概率也是可忽略的。故主动攻击者计算出群组密钥的概率可忽略。

综上所述,本方案具有认证性。

定理 2. 群组密钥管理方案是后向保密的。

证. 根据方案描述,当一个 LEO 卫星结点退出群组后,其所在簇的簇头 MEO 卫星改变自己对群组密钥的秘密贡献值,所有结点均生成新的群组密钥。新的密钥计算过程产生的中间值为 $T = T_0 \cdot e(P, P)^{a^*}$,其中 T_0 为原密钥计算过程的中间值。由于 a^* 是 Z_q^* 上的随机值, 所以对于该 LEO 卫星而言, T 也是一个随机值。该 LEO 卫星对新密钥的计算能力不强于外部攻击者的能力,根据定理 1,该 LEO 卫星计算出新密钥的概率可忽略,即方案具有后向保密性。

定理 3. 群组密钥管理方案是前向保密的。

证. 根据方案描述,当一个 LEO 卫星结点加入群组,其所在簇的簇头结点改变了自己对群组密钥的秘密贡献值,所有结点均生成新的群组密钥。新的密钥计算过程产生的中间值 T 和该 LEO 卫星结点加入前的中间值 T_0 满足 $T_0 = T \cdot e(P,P)^{-a^*}$。其中 T_0 为原密钥计算过程的中间值。由于 a^* 是 Z_q^* 上的随机值,T_0 对于该 LEO 卫星结点而言是一个随机值,该结点对加入前密钥的计算能力不强于外部攻击者的能力。根据定理 1,该结点计算出加入前密钥的概率可忽略,即方案具有前向保密性。

5　仿真实验与结果分析

为分析本文方案在空间信息网中的通信效率,利用 STK 卫星仿真软件(版本:8.0)和 OPNET 网络仿真软件(版本:14.5 教育版)将本文方案与经典的分布式密钥管理方案 G-DH[3]及 TDH1[4]在性能上进行仿真比较,并对密钥建立所需时间和密钥管理方案的通信开销进行评估。

在仿真场景中,空间信息网的卫星结点分为 MEO 层和 LEO 层卫星。为说明仿真结果的有效性,仿真实验中通过逐渐增加 LEO 卫星数目实现网络规模的逐渐增大,并在不同网络规模下分析密钥管理方案的效率。仿真参数的取值见表 1。

表 1　仿真参数设置

Table 1　Parameters for simulation

参数	值
MEO 轨道数	2
MEO 卫星数/轨道	8
MEO 卫星高度	10355km
MEO 轨道倾角	45°
MEO 星座类型	Walker Delta 星座
LEO 卫星数/轨道	10
LEO 卫星高度	1400
LEO 轨道倾角	86°
LEO 星座类型	Walker Polar 星座
群组密钥更新周期	4 小时

图 2 对比了在成员注册阶段完成后,不同网络规模情况下三种密钥管理方案建立密钥所需的时间。由图 2 可知,在不同网络规模下,本文方案建立一个新密钥所需的时间较另两个方案少;另一方面,随着网络规模增大,本文方案建立密钥所需时间的增长率较另外两个方案也更小。

图 3 对比了在 24 小时仿真中,使用不同密钥管理方案的系统通信量,这体现了不同密钥管理方案带来的通信开销的对比。如图 3 所示,在网络规模增大时,本文方案的系统通信开销显著小于对比方案。这是因为一方面 G-DH 密钥管理方案没有利用空间信息网的分层特点,网络中建立密钥时需要所有结点之间的交互,带来了极大的通信开销;而另一方面 TDH1 密钥管理方案虽然是分层式的,但是该协议中群组密钥的建立需要每个网络结点都对生成的密钥值有贡献,这在结点距离远,通信时延大的空间信息网中会带来很大的通信开销。本文方案利用

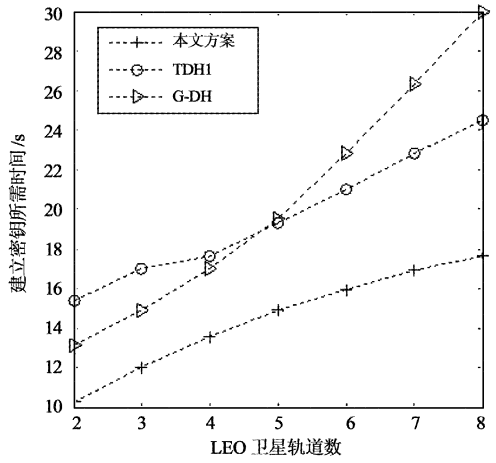

图2 密钥管理方案建立密钥所需的时间对比

Fig. 1 A comparison of time required to establish session key for different GKE schemes

了空间信息网的特点,群组密钥仅由簇头结点协商建立,无需 LEO 卫星参与,在网络规模增大时,依然能保持较低的通信开销,完全可以达到空间信息网对密钥管理协议的要求。

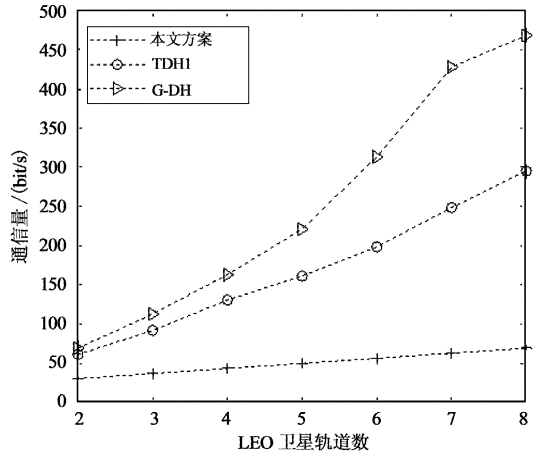

图3 密钥管理方案的通信量对比

Fig. 3 A comparison of communication overhead for different GKE schemes

6 结 论

本文提出了适用于 LEO/MEO 双层卫星结构空间信息网的基于身份群组密钥管理方案,针对空间信息网的特点,方案将所有卫星结点根据逻辑位置分为多个簇,MEO 卫星担任簇头,簇内结点为该 MEO 卫星能覆盖的 LEO 卫星。安全性分析表明,方案具有认证安全性,在网络结点发生变化时能够及时更新密钥,具有前向保密性和后向保密性。仿真实验表明,方案具有很高的通信效率。

参 考 文 献

[1] 刘小跃,马建峰,钟焰涛,等. 空间信息网安全组网新架构[J]. 网络安全技术与应用, 2009,6(6):13 -15. [Liu Xiao-yue, Ma Jian-feng, Zhong Yan-tao, et al. New construction for secure networking of space information networks[J]. Network Security Technology and Application, 2009, 6(6): 13 -15.]

[2] 吴廷勇,吴诗其. LEO/MEO 双层卫星网络层间星际链路建立策略的性能研究[J]. 电子与信息学报, 2008, 30(1): 67 -71. [Wu Ting-yong, Wu Shi-qi. Performance analysis of the inter-layer inter-satellite link establishment strategies in two-tier LEO/MEO satellite networks[J]. Journal of Electronics and Information Technology, 2008, 30(1): 67 - 71.]

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

[4] Manulis M. Provably secure group key exchange[D]. Bochum: Ruhr University,2007.

[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):553 -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] Shamir A. Identity-based cryptosystems and signature schemes[C]. The 4th International Cryptology Conference, New York, USA, August 19 -22, 1984.

[7] Goyal V. Reducing trust in the PKG in identity-based cryptoystems[C]. The 27th International Cryptology Conference, Santa Barbara, USA, August 19 -23,2007.

[8] Akyildiz I F, Ekici E, Bender M D. MLSR: a novel routing algorithm for multilayered satellite IP networks[J]. IEEE/ACM Transactions on Networking, 2002, 10(3): 411 - 424.

[9] Bao F, Deng R H, Zhu H. Variations of diffie-hellman problem[C]. The Fifth International Conference on Information and Communications Security, Huhehaote, China, October 10 - 13, 2003.

作者简介:钟焰涛(1980 -),男,博士,研究方向为信息安全与密码学。

通信地址:西安市太白南路2号西安电子科技大学171信箱(710071)

电话:(029)88207402

E-mail:zhongyantao@126.com

(编辑:余 未)