低轨卫星网络中基于轨道分簇的密钥更新算法

张志强[①] 张永健[②] 王 宇[③] 卢 昱[④]
[①](装备指挥技术学院研究生管理大队 北京 101416)
[②](国际关系学院信科系 北京 100091)
[③](装备指挥技术学院信息装备系 北京 101416)
[④](军械工程学院训练部 石家庄 050003)

摘 要：该文提出一种基于轨道分簇的低轨(LEO)卫星网络密钥更新算法，即 RAOC 算法。该算法根据运行轨道特性对 LEO 卫星网络进行分簇，通过动态产生密钥更新发起节点和簇首节点完成 LEO 卫星网络的密钥更新。RAOC 算法提出一种基于密钥更新锁的密钥更新状态描述方法，以确保密钥更新的一致性。仿真结果表明，与目前 LEO 卫星网络基于地基测控网和天基测控网的密钥更新算法相比，RAOC 算法能自主完成 LEO 卫星网络的密钥更新，并能提高 LEO 卫星网络密钥更新的效率。

关键词：卫星网络；LEO 星座；轨道分簇；密钥更新
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2010)03-0687-06
DOI: 10.3724/SP.J.1146.2009.01085

Rekeying Algorithm Based on Orbital Cluster in the LEO Satellite Network

Zhang Zhi-qiang[①] Zhang Yong-jian[②] Wang Yu[③] Lu Yu[④]
[①](*Company of Postgraduate Management*, *Academy of Equipment Command and Technology*, *Beijing* 101416, *China*)
[②](*Department of Information Technology*, *University of International Relations*, *Beijing* 100091, *China*)
[③](*Department of Information and Equipment*, *Academy of Equipment Command and Technology*, *Beijing* 101416, *China*)
[④](*Department of Training*, *Ordnance Engineering College*, *Shijiazhuang* 050003, *China*)

Abstract: A kind of Rekeying Algorithm based on Orbital Cluster (RAOC) is proposed in the Low Earth Orbit (LEO) satellite network. The LEO satellite network is divided into different clusters according to the characteristics of the LEO satellite network in RAOC. The rekeying process is carried out by the initiating node of the LEO satellite network and the head nodes of the clusters. Rekeying lock is introduced to ensure consistency of the rekeying. The simulation results indicate that RAOC can accomplish the rekeying automatically compared with ground-based TT&C(Tracking, Telemetry and Command) algorithm and space-based TT&C algorithm, and the rekeying efficiency is improved by RAOC.

Key words: Satellite network; LEO constellation; Orbital cluster; Rekeying

1 引言

低轨(LEO)卫星系统由于具有低时延和地面移动终端低功耗的特点[1]，可在通信、遥感等多个领域提供话音、图像等实时交互业务[2,3]。由于卫星通信的暴露特性[4]，卫星网络很容易受到安全攻击[5,6]。地面非授权用户可能对卫星通信进行窃听，并可能向卫星节点注入恶意信息，威胁卫星系统的安全。空间数据系统咨询委员会(Consultative Committee for Space Data Systems，CCSDS)分析了卫星网络的安全威胁，并提出了多种安全策略确保卫星网络的安全[5]。为防止恶意攻击造成卫星网络的灾难性破坏，目前采取了多种安全措施，如安全认证[7]、安全路由[8]、虚拟专网(VPN)[9]等，但这些安全措施是以密钥安全为前提和基础的。卫星在发射前分发的密钥有一定的生存期，必须经常对卫星密钥进行更新以保证卫星网络的安全。密钥更新是卫星网络安全研究的核心内容，也是关键技术难题[10]。

本文基于运行轨道把 LEO 卫星网络划分成不同的区域，提出基于轨道分簇的密钥更新算法(Rekey Algorithm based on Orbital Cluster,

2009-08-13 收到，2009-11-26 改回
国家 863 计划项目(2006AA701305)资助课题
通信作者：张志强 spreadzhiq.iang@foxmail.com

RAOC)。该算法主要通过分簇方法完成 LEO 卫星网络密钥更新，以提高 LEO 卫星网络的密钥更新效率，并降低 LEO 卫星网络密钥更新过程中对地面测控站的依赖。

2 LEO 卫星网络的现有密钥更新算法

文献[7,11,12]分析了卫星网络节点之间的密钥分发问题；文献[13]根据网络节点功能把天基网划分为不同的簇，从而对天基网密钥进行管理和更新；但现有文献缺乏结合卫星网络拓扑结构特点对卫星网络密钥管理进行分析。目前 LEO 卫星网络的密钥更新由地面测控站依次对每颗卫星进行密钥更新的方法完成，而专门针对 LEO 卫星网络的密钥更新研究相对较少。

2.1 LEO 卫星网络模型

LEO 卫星网络如图 1 所示，该网络中有 6 个极地轨道，每个轨道上有 11 颗卫星。由于采用定向天线进行通信，在具有星间链路的 LEO 卫星网络中，卫星节点一般只与邻居节点直接建立星间链路。

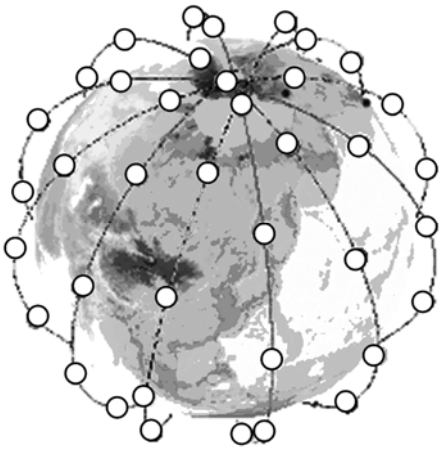


图 1 低轨卫星网络模型

2.2 基于地基测控网的 LEO 卫星网络密钥更新

地基测控网由地球上的测控站、测控船、航天控制中心、通信链路等组成[14,15]。基于地基测控网对低轨卫星网络进行测控时，由于受到地球曲率的限制，卫星通过测控站的时间很短，即使在全球范围内布站，地面测控网对卫星的测控覆盖率不超过 20%。对于地基测控网，可通过租用他国测控站的方法来提高测控覆盖率，但租用他国测控站，缺乏自主性和灵活性，往往受政治因素的影响，给密钥的更新造成极大威胁。目前通常通过少量的地面站对低轨星座进行密钥管理。如铱系统主要通过建在加拿大的两个地面测控站对系统进行测控和管理。基于地基测控网的 LEO 卫星网络的密钥更新周期与 LEO 卫星节点的轨道周期有直接关系。

2.3 基于天基测控网的 LEO 卫星网络密钥更新

目前测控网正由地基向天基发展，由 3 颗地球同步轨道构成的天基测控网可为多颗低轨卫星提供近连续覆盖[14,16]。通过 1 颗或 2 颗地球同步轨道卫星转发，与一个地面测控站相配合，可实现 LEO 卫星网络节点的实时密钥更新。基于天基测控网对 LEO 卫星网络进行密钥更新，可大大缩短密钥更新时间。

基于地基测控网和天基测控网对 LEO 卫星网络进行密钥更新，需要与地面站进行多次通信，对地面站的依赖程度较大。当地面测控站因地震、战争或其他因素被毁时，LEO 卫星网络的密钥更新将受到严重影响，现有密钥更新方法已不能适应卫星网络自主管理的发展需要。

3 RAOC 密钥更新算法分析

本文提出的 RAOC 算法由密钥更新锁机制、密钥动态分发机制和入侵容忍机制构成。密钥更新锁机制确保 LEO 卫星网络密钥更新的一致性。密钥动态分发机制通过改进的 Beller-Yacobi 协议[12]把密钥安全传递到 LEO 卫星网络的每个节点。入侵容忍机制确保 LEO 卫星网络被攻击时的密钥更新安全性。RAOC 算法的密钥更新总体过程如图 2 所示。RAOC 算法首先动态产生密钥更新发起节点及簇首节点，通过密钥更新锁逐级控制密钥的分发，LEO 卫星网络所有节点密钥更新完成后，密钥更新发起节点向地面测控站发送确认信号。

3.1 RAOC 算法密钥更新锁机制

(1)密钥更新锁设置　本文中 $L(i,j)$ 表示轨道 i

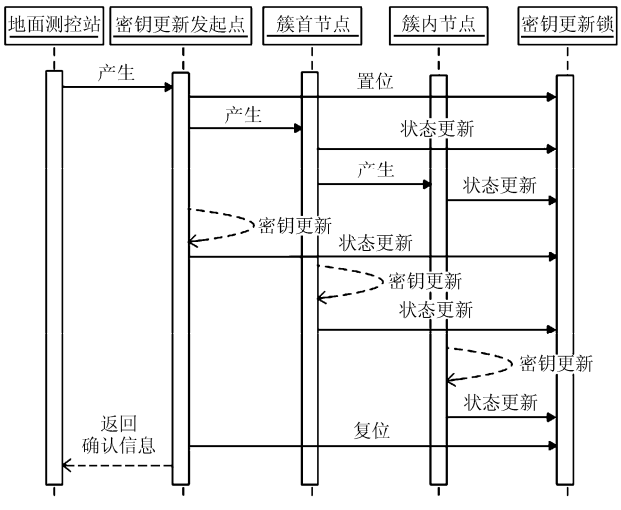


图 2 RAOC 密钥更新算法总体过程

内的第 j 个卫星节点，与 $L(i,j)$ 具有相同运行轨道的卫星节点集合记为簇 $C(i)$。RAOC 密钥更新锁由 $A_0A_1A_2A_3A_4$ 5 位二进制位标识，A_0A_1 表示节点的种类，$A_2A_3A_4$ 表示节点密钥更新状态。为便于描述，节点 $L(i,j)$ 的密钥锁表示为 S_{ij}，S_{ij} 的具体含义如表 1 所示。

表 1 密钥更新锁具体含义

S_{ij}	含义
00000	簇内节点密钥更新完成
00001	簇内节点密钥更新执行
10111	簇首节点密钥更新执行
10110	簇首节点密钥更新完成
10000	簇首所在簇密钥更新完成
11111	密钥更新发起节点密钥更新执行
11110	密钥更新发起节点密钥更新完成
11100	密钥更新发起节点所在簇密钥更新完成
11000	网络所有节点密钥更新完成

(2)密钥更新状态转换　图 3 描述了 RAOC 算法的密钥更新状态转换图。LEO 卫星网络密钥更新前，所有节点状态均为 00000。A_0A_1 变化表示节点角色的转换，$A_2A_3A_4$ 变化表示节点密钥更新状态的转变。簇内节点 $A_2A_3A_4$ 的变化反映本节点的密钥更新情况；簇首节点 $A_2A_3A_4$ 的变化反映簇首节点及本簇节点的密钥更新情况；密钥更新发起节点 $A_0A_1A_2A_3A_4$ 的变化反映簇首和整个网络的密钥更新情况。LEO 卫星网络密钥更新完成后，$A_0A_1A_2A_3A_4$ 将全部置 0，表示可进行下一轮的密钥更新。

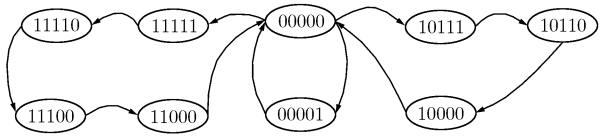


图 3 RAOC 密钥更新状态转换图

3.2 RAOC 算法密钥动态分发机制

(1)密钥更新的发起　RAOC 算法选择与地面测控站可见时间较长的 LEO 卫星网络节点作为密钥更新发起节点，该节点记为 $L(m,n)$，$L(m,n)$ 密钥更新锁初始化为 11111。LEO 卫星网络密钥更新开始前，首先对网络所有节点的密钥更新状态 S_{ij} 进行二进制或运算，$M=\sum_{i=1}^{6}\sum_{j=1}^{11}S_{ij}$。若 $M=00000$，则卫星网络处于密钥更新等待状态，可以对卫星网络发起密钥更新，否则不能对卫星网络发起密钥更新。$L(m,n)$ 密钥更新完成后，密钥更新锁更新为 11110。

(2)簇首节点密钥更新　$L(m,n)$ 所在簇的簇首节点为 $L(m,n)$，选择 $L(i,n)\{i|i\neq m,i\in\{1,2,3,4,5,6\}\}$ 为其他簇的簇首节点，$L(i,n)$ 节点的密钥更新锁初始化为 10111。计算 $M=\sum_{n=1}^{6}(S_{mn}\cdot 00001)$，若 M=00000，则全部簇首节点密钥更新已完成。$L(i,n)$ 节点密钥更新完成后，密钥更新锁更新为 10110，$L(m,n)$ 节点密钥更新锁更新为 11100。

(3)簇内节点密钥更新　簇内节点的密钥更新由簇首节点控制执行，簇首节点密钥更新锁在本簇节点密钥更新完成后更新为 10000。对各簇首节点的密钥更新锁 S_{ij} 进行二进制或运算，$M=\sum_{j=1}^{6}(S_{ij}\cdot 00111)$，若 M=00000，则各簇节点的密钥更新已完成。簇内所有节点密钥更新完成后，各簇首节点的密钥更新锁更新为 00000，密钥更新发起节点的密钥更新锁更新为 11000，通过星间链路向地面测控站发送密钥更新确认信号，并把密钥更新锁更新为 00000，LEO 卫星网络的密钥更新过程完成。

3.3 RAOC 算法入侵容忍机制

(1)密钥更新发起节点　RAOC 算法通过秘密共享的方法防止密钥更新发起节点被攻击后对 LEO 卫星网络造成安全威胁。密钥更新发起节点对 LEO 卫星网络发起密钥更新前，通过发送授权密钥加密的秘密信息以证明其未遭攻击。授权密钥通过秘密共享的方法提前分发给 LEO 卫星网络中的每个节点，具体算法参照文献[17]，本文选择门限值为 5。密钥更新发起前，密钥更新发起节点需要与 4 个邻居节点进行通信，以获取秘密份额，从而生成授权密钥，以获得地面测控站的授权。如果密钥更新发起节点遭到攻击，将不能获取邻居节点的秘密份额，从而无权发起 LEO 卫星网络的密钥更新。

(2)簇首、簇内节点　RAOC 算法通过隔离机制确保簇首、簇内节点遭到攻击后 LEO 卫星网络的安全。簇首或簇内节点 $L(i,j)$ 被入侵后，地面将对 $L(i,j)$ 的邻居节点 $L(i-1,j)$，$L(i+1,j)$，$L(i,j+1)$，$L(i,j-1)$ 发送与节点 $L(i,j)$ 终止通信的指令，$L(i,j)$ 邻居节点将终止与 $L(i,j)$ 节点的通信，被攻击节点将被隔离，从而不能获取 LEO 卫星网络的更新密钥。簇首节点被隔离后，将选取相同簇内的邻居节点作为新簇首节点。

4　算法仿真及性能分析

本文基于 NS2, STK(Satellite Tool Kit),

MATLAB 搭建的仿真平台对 3 种密钥更新算法进行了仿真分析，仿真过程中节点之间密钥的传递统一采用改进的 Beller-Yacobi 协议。在高纬度地区设立一个测控站，具体位置为北纬 70°，西经 118°。LEO 网络参照铱系统进行设置，轨道高度为 780 km，轨道面数量为 6，同一轨道卫星数量为 11，每颗卫星星间链路数为 4。

4.1 地基测控网密钥更新算法仿真

通过在高纬度地区设立的测控站，可同时测控 6 个轨道的多颗卫星。因 6 个轨道具有相同的轨道运行周期，每个轨道面内的卫星与地面测控站的可见性规律相同。图 4 显示了一个轨道运行周期地面测控站与第 1 轨道面内 11 颗卫星的可见时间。从图中可以看出，同一时刻同一轨道面内与地面测控站可见的卫星数为 2。地面测控站与 LEO 卫星传递密钥的时间为 30 ms 左右，LEO 卫星网络的密钥更新时间主要取决于 LEO 卫星的轨道运行周期。

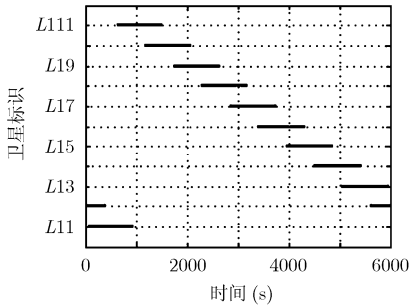


图 4 一个轨道周期地面站与卫星的可见性分析

4.2 天基测控网密钥更新算法仿真

基于天基测控网的 LEO 卫星网络密钥更新仿真，首先估算密钥更新的总体时间，然后分析该段时间内 LEO 卫星与 G_1, G_2, G_3 的可见性，可见性分析场景如图 5 所示。

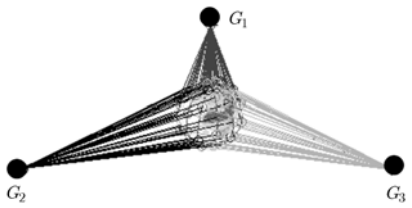


图 5 静止轨道卫星与 LEO 卫星的可见性分析场景

可见性矩阵用 $\boldsymbol{V}$ 表示，$\boldsymbol{V}(i,j)\in\{1,2,3\}$，分别表示与卫星 $L(i,j)$ 可见的静止轨道卫星为 G_1, G_2, G_3。可见性矩阵如下：

$$\boldsymbol{V}=\begin{bmatrix}1&1&2&2&2&2&2&2&2&2&1\\2&2&2&2&2&2&2&2&2&2&2\\2&2&2&2&3&3&3&1&2&2&2\\2&2&2&1&1&1&1&1&2&2&2\\2&2&2&2&1&1&1&1&2&2&2\\2&2&2&1&1&1&1&2&2&2&2\end{bmatrix}$$

LEO 卫星网络密钥更新平均时间矩阵用 $\boldsymbol{T}$ 表示，$\boldsymbol{T}(i,j)$ 表示 $L(i,j)$ 的密钥更新平均时间，$\boldsymbol{T}(i,j)$ 的时间单位为秒。基于天基测控网的密钥更新平均时间矩阵如下：

$$\boldsymbol{T}=\begin{bmatrix}1.4459&1.4611&0.8045&0.7846&0.7666&0.7570&0.7594&0.7729&0.7925&0.8115&1.4576\\0.7904&0.7889&0.7888&0.7903&0.7928&0.7955&0.7975&0.7983&0.7976&0.7955&0.7929\\0.7530&0.7579&0.7743&0.7960&1.4706&1.4480&1.4513&1.5400&0.8019&0.7799&0.7614\\0.7269&0.7490&0.7839&1.5248&1.5208&1.5176&1.5163&1.5173&0.7847&0.7497&0.7272\\0.7165&0.7313&0.7657&0.8058&1.4963&1.4817&1.4809&1.4942&0.8009&0.7608&0.7281\\0.7378&0.7591&0.7901&1.4934&1.4631&1.4523&1.4660&0.8120&0.7808&0.7515&0.7348\end{bmatrix}$$

通过对矩阵 $\boldsymbol{V}$ 和矩阵 $\boldsymbol{T}$ 对比分析可以看出，与 G_2 可见的 LEO 卫星密钥更新时间相对较短，而与 G_1 和 G_3 可见的 LEO 卫星密钥更新时间相对较长。这主要是因为地面测控站与 G_2 可见，与 G_2 可见的 LEO 卫星通过一次转发就可完成密钥更新，而与 G_1 和 G_3 可见的卫星，由于需要两次转发才能完成密钥更新。

4.3 RAOC 算法仿真

RAOC 算法的仿真场景如图 6 所示，通过随机设定仿真开始时间，以仿真地面测控站对 LEO 卫星网络的随机接入，根据设定的仿真开始时间，选择与地面测控站可见时间较长的 LEO 卫星作为密钥更新发起节点，选择其他轨道面内与该节点编号相同的节点为簇首节点，根据仿真时间实时计算 LEO 卫星网络节点之间的距离，并结合密钥传输协议计算 RAOC 密钥更新时间。在仿真过程中，邻居节点之间距离的变化规律如图 7 所示，同一轨道内的邻居节点之间距离保持不变，相邻轨道间的邻居节点之间距离呈周期性变化，密钥传递时间根据传输距离计算获得。

4.4 仿真结果分析

在仿真过程中，共进行 1000 次测试，每 100 次

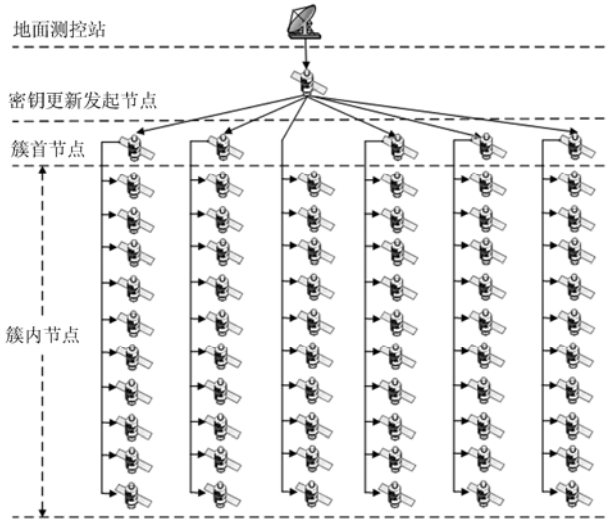


图 6 RAOC 密钥更新算法仿真过程图

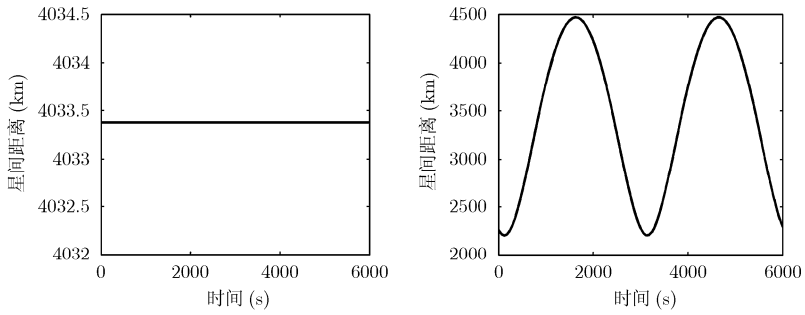
测试取一次平均值，仿真结果如图 8 所示。

(1)密钥更新时间　图 8 所示的仿真结果显示，基于地基测控网的密钥更新平均时间为 5572 s，基于天基测控网的密钥更新平均时间为 64 s，RAOC 密钥更新算法的平均时间为 5.62 s。和基于地基和天基测控网的密钥更新算法相比，RAOC 密钥更新算法具有较高的更新效率。基于地基测控网的密钥更新算法由于受与地面测控站可见性的影响，密钥更新时间接近于轨道周期。基于天基测控网的密钥更新算法因密钥更新过程中通信距离较长，密钥更新时间相对较长，而 RAOC 算法中密钥更新过程中节点之间的通信距离较短，且相邻节点可保持实时可见，密钥更新时间相对较短。

(2)安全性分析　在相同的传输环境中，RAOC 算法与地基测控网密钥更新算法和天基测控网密钥更新算法面临相同的安全威胁，由于节点之间的密钥传输均采用改进的 Beller-Yacobi 协议，RAOC 算法与其他两种密钥更新算法节点之间的密钥传输具有相同的安全性。RAOC 算法通过秘密共享的方法对密钥更新发起节点进行授权，以防止其被攻击后对 LEO 卫星网络发起密钥更新。对于簇首节点和簇内节点，通过隔离的方法阻止被入侵节点获取更新密钥，从而保证了 LEO 卫星网络其他节点的安全。RAOC 算法与地基测控网和天基测控网密钥更新算法相比，具有相同的密钥更新安全性。

5　结论

现有的密钥更新算法不能适应 LEO 卫星网络自主管理的发展需求。本文根据 LEO 低轨卫星网络的组网特点，针对 LEO 卫星网络密钥更新过程对地面测控站依赖程度较大的问题，提出了一种基于轨道分簇的密钥更新算法，即 RAOC 算法。该算法根据运行轨道对卫星网络进行分簇，通过动态选择密钥更新发起节点和簇首节点，在地面测控站发出密钥更新指令后，可自主完成 LEO 卫星网络的密钥更新，并通过密钥更新锁来解决密钥更新过程中的冲突问题。仿真结果表明 RAOC 算法可行，并具有较高的更新效率。该算法对于未来中低轨星座的建设有一定的借鉴意义。



(a) 同一轨道内邻居节点的距离变化图　(b) 相邻轨道邻居节点的距离变化图

图 7 邻居节点随时间的距离变化图

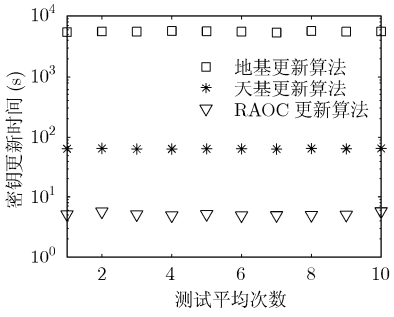


图 8 RAOC 算法与现有 LEO 密钥更新算法性能对比测试图

参 考 文 献

[1] Vladimirova T, Wu X H, and Bridges C P. Development of a satellite sensor network for future space missions[C]. 2008 Aerospace Conference, Big Sky, MT，Mar.1–8, 2008: 1–10.

[2] Vladimirova T and Sidibeh K. WLAN for earth observation satellite formations in LEO[C]. Proceedings of the 2008 Bio-inspired, Learning and Intelligent Systems for Security, Edinburgh, Scotland, UK, Aug, 4–6, 2008: 119–124.

[3] Yang D N and Liao W. On multicast routing using rectilinear steiner trees for LEO satellite networks[J]. *Vehicular Technology*, 2008, 57(4): 2560–2569.

[4] CCSDS 350.0-G-2. The application of CCSDS protocols to

secure systems[S]. Washington, DC, USA, 2006.

[5] CCSDS 350.1-G-1. Security threats against space missions[S]. Washington, DC, USA, 2006.

[6] CCSDS 350.4-G-1.CCSDS guide for secure system interconnection[S]. Washington. DC, USA, 2007.

[7] Chayan D, Lalitkrushna T, and Annie N, *et al*.. A new encryption-decryption scheme that solves key management problem in remote sensing satellite[C]. First International Conference on Emerging Trends in Engineering and Technology, Nagpur, Maharashtra, India, Jul.16–18, 2008: 1261–1266.

[8] 李喆, 刘军. 卫星网络安全路由研究[J]. 通信学报, 2006, 27(8): 113–118.
Li Z and Liu J. Research on secure routing algorithm in satellite networks[J]. *Journal on Communications*, 2006, 27(8): 113–118.

[9] Parichehreh A and Eliasi B. VPN over satellite: performance improving of E2E secured TCP flows[C]. 5th IFIP International Conference on Wireless and Optical Communications Networks, Surabaya, Indonesia, May. 5–7, 2008: 1–4.

[10] CCSDS 350.3-G-1. Authentication/integrity algorithm issues survey[S]. Washington. DC, USA, 2008.

[11] Roy-Chowdhury A, Baras J S, and Hadjitheodosiou M, *et al*.. Security issues in hybrid networks with a satellite component[J]. *IEEE Wireless Communications*, 2005, 12(6): 50–61.

[12] Ji Y X, Ma H T, and Zheng G. Analysis and design on key updating policies for satellite networks[J]. *International Journal of Computers, Communications and Control*, 2008, 3(4): 343–352.

[13] Balasubramanian A, Mishra S, and Sridhar R. Secure key management for NASA communication. http://gltrs.grc.nasa.gov/reports/2005/cp-2005-213878. 2009. 8.

[14] 于志坚. 我国航天测控系统的现状与发展[J]. 中国工程科学, 2006, 8(10): 41–46.
Yu Z J. Status quo and development of spaceflight TT&C systems[J]. *Engineering Science*, 2006, 8(10): 41–46.

[15] 杨永安, 冯祖仁. 陆基 S 频段测控网卫星仿真现状与发展研究[J]. 系统仿真学报, 2004, 16(12): 2636–2639.
Yang Y A and Feng Z R. Study of current status and development trend of the ground-base S-band TT&C network satellite simulation in China[J]. *Journal of System Simulation*, 2004, 16(12): 2636–2639.

[16] 杨天社, 董小社, 席政等. 低轨航天器天基测控方法研究[J]. 空间科学学报, 2007, 27(3): 245–249.
Yang T S, Dong X S, and Xi Z, *et al*.. Space-based TTC method of lower orbit satellite[J]. *Chinese Journal of Space Science*, 2007, 27(3): 245–249.

[17] 李慧贤, 庞辽军. 基于双线性变换的可证明安全的秘密共享方案[J]. 通信学报, 2008, 29(10): 47–48.
Li H X and Pang L J. Provably secure secret sharing scheme based on bilinear maps[J]. *Journal on Communications*, 2008, 29(10): 47–48.

张志强： 男，1974 年生，博士生，研究方向为卫星组网安全.

王 宇： 男，1971 年生，副教授，硕士生导师，研究方向为信息网络安全和网络控制.

卢 昱： 男，1960 年生，教授，博士生导师，研究方向为空间信息对抗.