新的低轨星座组网认证与群组密钥协商协议

张子剑[1]，周琪[1]，张川[1]，童逍瑶[1]，李春磊[2]，王龙[1]
（1. 北京理工大学计算机学院，北京 100081；2. 中国民航信息集团公司，北京 101318）

摘 要：由于低轨卫星具有通信和持续监测的功能，其在航天领域得到广泛的应用，然而现有的卫星通信系统中没有专门的认证系统。为了解决该问题，针对低轨星座组网设计了轻量级的认证协议，考虑了认证过程中链路切换的情况，对协议进行了仿真验证并与 3GPP AKA 协议进行对比。模拟实验结果表明，低轨星座组网认证协议比 3GPP AKA 协议效率提高了 20%，同时群组密钥协商时间约为 300 ms。

关键词：低轨卫星组网；认证；密钥协商
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018102

New low-earth orbit satellites authentication and group key agreement protocol

ZHANG Zijian[1], ZHOU Qi[1], ZHANG Chuan[1], TONG Xiaoyao[1], LI Chunlei[2], WANG Long[1]
1. School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China
2. China TravelSky Holding Company, Beijing 101318, China

Abstract: Due to the function of communication and continuous monitoring, the low-earth orbit satellites are widely used in the aerospace field. However, there is no special authentication protocol in the existing satellite communication system. In order to solve this problem, a lightweight authentication protocol which considering the switch of communication path in the authentication process was designed for the low-earth orbit satellites, and the proposed protocol was verified by simulation and compared with the 3GPP AKA protocol. The simulation results show that the protocol has a 20% higher efficiency than 3GPP AKA protocol, and the spend of group key agreement protocol is about 300 ms.

Key words: low-earth orbit satellites, authentication, key agreement

1 引言

在低轨星座组网中，卫星数目相对较多，如铱星通信系统中一共有 66 颗低轨卫星，全球星通信系统中一共有 48 颗低轨卫星。同时，低轨星座组网中卫星的用途广泛[1]，由于低轨卫星距离地面很近，其广泛用于检测和通信。

然而，现有的卫星系统大多都是由单颗卫星组成的。目前，国外的卫星组网仅有铱星通信系统和全球星通信系统。由于低轨星座组网的实现和维护成本较高，实现代价较大，国内并没有成熟的低轨星座组网。

针对低轨星座组网，国内外许多学者对其认证协议进行了研究。张小亮等[2]设计了一种端到端认证协议并构建了安全认证仿真系统。徐志博等[3]基于 IKE 协议设计了一种适用于卫星网络的端到端认证协议。徐日新等[4]为卫星移动通信系统提出了一种结合可穿戴设备与智能终端的持续认证方案。高婧等[5]针对传统认证方案中认证效率较低、认证过程较复杂等问题提出了一种基于 ELGmamal 数字签名的卫星网络认证方案。Cruickshank[6]设计了一种基于 PKI（public key infrastructure）架构的用户与卫星间双向认证的协议。Chen 等[7]在总结一些认

收稿日期：2017-10-27；**修回日期**：2018-05-02
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800301）
Foundation Item: The National Key Research and Development Program of China (No.2016YFB0800301)

证协议不足的基础上提出了一种自验证的认证协议。然而，由于低轨星座组网中存在 2 条相邻但卫星运行方向相反的轨道，相邻轨道间的卫星无法进行稳定的通信，需要进行链路切换，比如通过同一轨道内的低轨卫星经过高纬度地区将消息发送至目标关口站。这样的特性使低轨星座组网具有拓扑动态变化高、链路切换快的特点，目前的认证协议不适用于低轨星座组网。同时，针对低轨星座组网，现有的认证协议不够安全。

本文创新点如下：1) 针对低轨卫星组网设计了轻量级认证协议，该认证协议考虑到低轨星座组网拓扑动态变化高、链路切换快的特点；2) 采用了基于群组的密钥协商协议，提高了组网通信的效率；3) 通过仿真实验模拟了低轨星座组网认证协议以及群组密钥协商协议，并对协议的安全性以及性能进行了分析。

2　相关工作

针对组网认证，本文首先研究了 3GPP 协议。3GPP 在移动通信领域提出了一系列的认证协议，研究 3GPP 相关的认证协议可以为卫星认证提供参考价值，因此，国内有大量研究人员对加密和认证协议进行了相关研究。其中，西安邮电大学的赖成喆等[8]基于 3GPP 标准框架和技术，对现有的 3GPP 认证和密钥协商协议进行了分类概述和讨论，并对未来技术的发展进行展望。Gai 等[9]提出了一种基于张量的完全同态加密算法，保证加密数据的安全性。陆峰等[10]基于 3GPP AKA 协议安全框架提出了一种新的认证与密钥协商协议。装备学院的周赤等[11]研究了 4G 通信主流技术 LTE，针对 LTE 存在的安全问题提出了一种多路径策略。该策略能够通过将网络编码和 TCP 进行最大化融合提高网络的利用率。

Zhang 等[12]指出 3GPP AKA 协议存在重定向攻击等安全问题，并提出了增强型 AP-AKA 协议。针对 Zhang 等[12]提出的增强型 AP-AKA 协议的不足，Juang 等[13]采用临时密钥体制完善协议，解决了 IMSI 标识暴露、交互信息流量大以及存储节点存储负担重等问题；Lee 等[14]针对 AP-AKA 协议的效率问题，提出了解决方法，在保证安全性的基础上提高了 AP-AKA 的效率。由于 3GPP 中存在重定向攻击等安全问题，本文提出了一种适应于低轨星座组网的轻量级认证协议。

针对群组密钥协商协议，Diffie 等[15]最早提出的密钥协商协议仅支持 2 个参与者。Joux[16]基于 Weil 对实现了 3 个参与者的密钥协商协议。然而，这些协议在群成员较多或通信时延较长时效率较低，也无法抵御“中间人攻击”。针对这些不足，许多学者提出了一些新的协议。陈虹等[17]采用双线性对运算方法提出了一种改进的基于身份的认证密钥协商协议。陈海红等[18]基于 Weil 对和完全三叉树提出了一种新的群组密钥协商协议。

3　基础知识

现有的移动通信系统安全框架采用的是 3GPP 组织建议的 AKA 协议机制。通过研究 3GPP 标准文档[19]，3GPP AKA 协议的具体流程如图 1 所示。

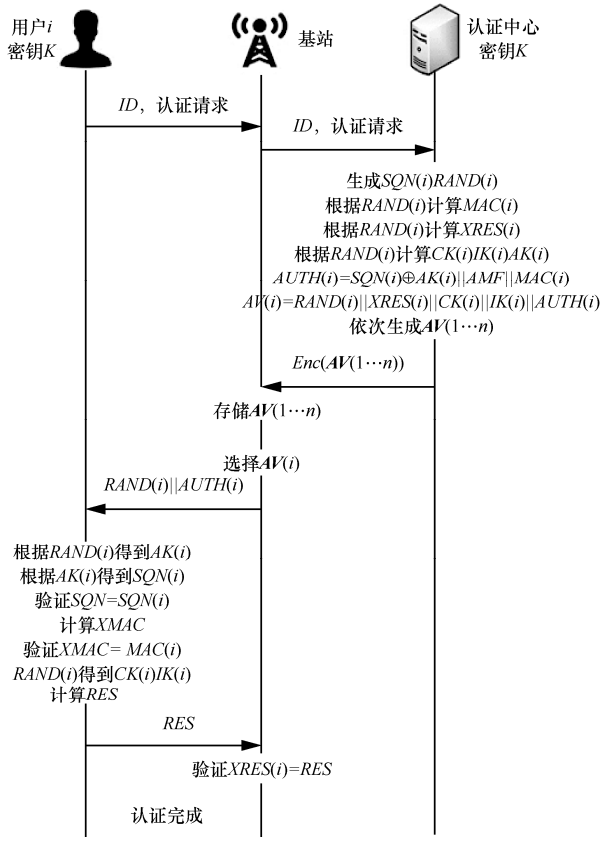


图 1　3GPP AKA 协议流程

在 3GPP AKA 协议中，认证向量 ***AV*** 由 5 个部分组成，分别是随机数 *RAND*、用于验证用户的 *XRES*、用于加密的密钥 *CK*、用于完整性验证的密钥 *IK* 以及用于认证检验的 *AUTH*。生成认证向量 ***AV*** 的算法如算法 1 所示。其中，f_0 是伪随机数发生器，用于产生伪随机数，f_1、f_2 是消息认证码算法，f_3 是加密密钥生成算法，f_4 是完整性密钥生成算法，f_5 是匿名密钥生成算法。

算法 1 3GPP AKA 认证向量生成算法

输入 主密钥 K

输出 认证向量 $\boldsymbol{AV}$

$MAC = f_{1_K}(SQN \| RAND \| AMF)$

$XRE = f_{2_K}(RAND)$

$CK = f_{3_K}(RAND)$

$IK = f_{4_K}(RAND)$

$AK = f_{5_K}(RAND)$

$AUTH = SQN \oplus AK \| AMF \| MAC$

$\boldsymbol{AV} = RAND \| XRES \| CK \| IK \| AUTH$

return $\boldsymbol{AV}$

用户收到认证请求应答时，根据得到的 $RAND(i)$ 以及 $AUTH(i)$对基站的身份进行认证。认证如算法 2 所示。

算法 2 3GPP AKA 用户认证基站算法

输入 $RAND||AUTH$

输出 认证结果

$AK = f_{5_K}(RAND)$

$SQN = (SQN \oplus AK) \oplus AK$

$XMAC = f_{1_K}(SQN \| RAND \| AMF)$

if $XMAC = MAC$ then

return true

else

return false

end if

用户认证基站成功后，需要通过 $CK = f_{3_K}(RAND)$ 以及 $IK = f_{4_K}(RAND)$ 得到加密密钥 CK 和完整性密钥 IK。与此同时，用户通过 $RES = f_{3_K}(RAND)$ 计算得到 RES。基站得到 RES 后只需检查 RES 和 $XRES$ 是否相等即可认证用户的身份。

4 低轨星座组网认证模型

低轨星座组网模型如图 2 所示。为了形式化说明低轨星座组网认证过程，首先给出低轨星座组网、低轨卫星、低轨星间链路以及低轨卫星关口站的符号化定义。

1) 低轨星座组网。LUG 表示低轨星座组网，它由低轨卫星以及低轨星间链路组成。低轨星座组网可以用无向属性图 $LUG = (LV, LE)$表示，其中，LV 表示低轨卫星，LE 表示低轨星间链路。

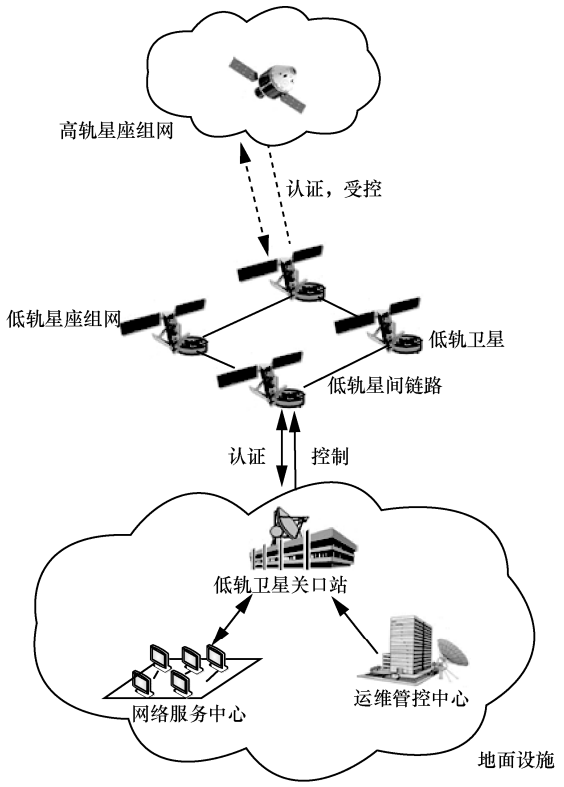


图 2 低轨星座组网模型

2) 低轨卫星。低轨卫星（LV）表示低轨星座组网中的低轨卫星，记为$<n^{LV}, s^{LV}, d^{LV}>$，其中，n^{LV} 表示低轨卫星编号，唯一标识一个低轨卫星；s^{LV} 表示低轨卫星的安全模块；d^{LV} 表示低轨卫星的受控模块。

3) 低轨星间链路。低轨星间链路 LE 表示低轨卫星之间的安全模块，记为$<lv_m, lv_n, s^{LE}>$，其中 $lv_m \in LV$ 为边 le 的起点，$lv_n \in LV$ 为边 le 的终点。

4) 低轨卫星关口站。低轨卫星关口站用 LS 表示，记为$<n^{LS}, s^{LS}, c^{LS}>$，其中，n^{LS} 表示低轨卫星关口站编号，唯一标识一个低轨卫星关口站；s^{LS} 表示低轨卫星的安全模块；c^{LS} 表示的是低轨卫星关口站的控制模块。

5 低轨星座组网认证与群组密钥协商协议

5.1 低轨星座组网认证协议

低轨星座组网节点间的认证，一方面，因为卫星经过极地交汇处之后相邻两侧轨道上的卫星发生了变化，相应的卫星间的通信链路需要进行切换，卫星之间也需要进行重新认证；另一方面，存在处于相邻轨道上但运行方向相反的卫星，这样的卫星之间不能直接进行通信，需要通过同轨道上的卫星往高纬度方

向进行通信再跳转至相邻轨道上，这样，链路上的卫星之间也需要进行认证。因此，需要研究出一种轻量级的认证协议，以满足低轨星座组网的认证需求。

低轨星座组网中低轨卫星的认证依赖地面的低轨卫星关口站进行认证。当低轨卫星 1 需要与低轨卫星 2 进行认证时，低轨卫星 1 首先会与低轨卫星关口站进行认证。认证成功后，低轨卫星关口站会根据低轨卫星 1 的认证请求选择相应的低轨卫星 2 进行认证。双方都认证完成后，由低轨卫星关口站产生对称密钥并分发给低轨卫星 1 和低轨卫星 2。此时，低轨卫星 1 与低轨卫星 2 已经完成了双方的互认证，它们使用低轨卫星关口站分发的对称密钥进行加密通信。认证过程如图 3 所示。

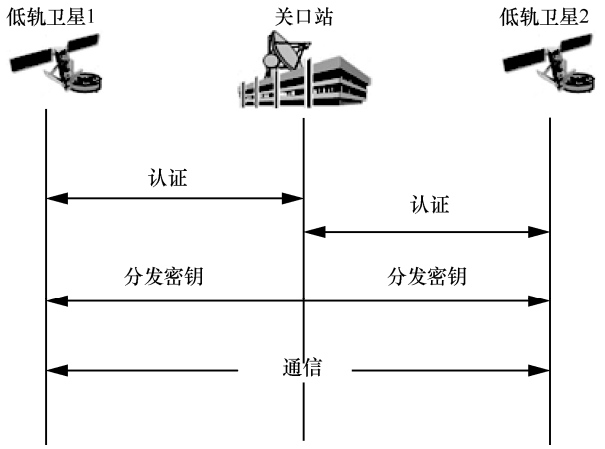


图 3　低轨星座组网认证流程

低轨卫星与关口站组网认证协议流程如图 4 所示，令 *PRNG* 为伪随机数发生器，*Enc* 为对称加密算法。

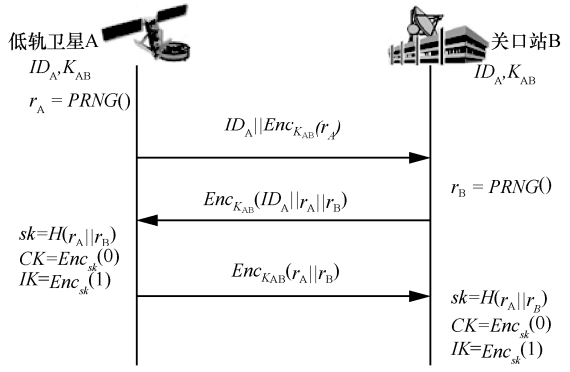


图 4　低轨卫星与关口站组网认证协议流程

1) 低轨卫星 A 发起认证请求前，读取关口站 B 的 ID_B 以及自己与关口站 B 的预共享密钥 K_{AB}。

2) 低轨卫星 A 产生随机数 $r_A = PRNG()$，并利用 K_{AB} 计算密文 $Enc_{K_{AB}}(r_A)$，然后发送 $ID_A \| Enc_{K_{AB}}(r_A)$ 给 B。

3) 关口站 B 收到了低轨卫星 A 发送的消息后，利用与 A 预共享的密钥解密密文获得 r_A，同时产生 r_B，将 $Enc_{K_{AB}}(ID_A \| r_A \| r_B)$ 发送给低轨卫星 A。

4) 低轨卫星 A 接收到关口站 B 的消息后，利用与 B 预共享的密钥解密密文，得到 ID_A、r_A、r_B，验证 ID_A、r_A 是否正确，计算 $sk = H(r_A \| r_B)$ 然后利用 sk 计算出 $CK = Enc_{sk}(0)$，再利用与 ID_B 的预共享密钥 K_{AB} 计算 $Enc_{K_{AB}}(r_A \| r_B)$，并将其发送给关口站 B。

5) 关口站 B 接收到低轨卫星 A 的消息后，利用与 A 预共享的密钥 K_{AB} 解密密文，得到 r_A、r_B，验证 r_A、r_B 是否正确，从而验证 A 的身份，并计算 $sk = H(r_A \| r_B)$，从而利用 sk 计算出 $CK = Enc_{sk}(0)$、$IK = Enc_{sk}(1)$。

考虑到星地传输时延较大，本文设计的协议只需要关口站和卫星 3 次消息传递即可完成认证，效率较高。

下面，使用符号化定义描述低轨星座组网认证过程。当低轨卫星 lv_i 需要加入低轨星座组网 LUG 时，它首先与低轨卫星关口站 ls_k 进行认证。与低轨卫星关口站 ls_k 完成认证之后，低轨卫星 lv_i 会向低轨卫星关口站 ls_k 发送与低轨卫星 lv_j 的认证请求。接下来，低轨卫星关口站 ls_k 将与低轨卫星 lv_j 进行认证。同时，低轨卫星关口站 ls_k 会生成低轨卫星 lv_i 与低轨卫星 lv_j 之间的会话密钥。当低轨卫星关口站与 2 个卫星认证通过后，低轨卫星关口站将会话密钥发送给低轨卫星 lv_i 和低轨卫星 lv_j。低轨卫星 lv_i 与低轨卫星 lv_j 完成认证后，低轨卫星 lv_i 将加入低轨星座组网 LUG 中，此时，低轨星座组网会增加与低轨卫星 lv_i 以及低轨卫星 lv_j 相关联的低轨星间链路 le_{ij}。当低轨卫星关口站需要控制低轨星座组网 LUG 时，低轨卫星关口站的控制模块 c^{LS} 与低轨卫星的受控模块 d^{LV} 对接。

由于低轨星座组网具有网络拓扑结构高动态变化、星际链路快速切换的特点，认证方案需要考虑认证时如何进行切换。

假设地面存在 3 个关口站，那么在本方案中，每个低轨卫星需要根据周围相邻的存在通信链路的低轨卫星与目标关口站地理位置的空间距离来决定下一跳低轨卫星。

以一条消息需要经过低轨星座组网转发进入地面关口站为例，图 5 为局部的低轨星座组网。

首先，消息从地面终端发往离终端最近的低轨卫星 Sat_{35}。低轨卫星 Sat_{35} 收到消息之后，会计算当前时刻低轨卫星 Sat_{45}、低轨卫星 Sat_{34} 以及低轨卫星 Sat_{25} 与关口站 2 的空间距离 s_1、s_2、s_3。由图 5 可以看出，s_2 最小，因此低轨卫星 Sat_{35} 优先选择向低轨卫星 Sat_{34} 发送消息。如果低轨卫星 Sat_{34} 失效，则向与关口站空间距离更远一些的 Sat_{25} 发送消息。如果 Sat_{25} 也失效，则向低轨卫星 Sat_{45} 发送消息。如果周围低轨卫星均已失效，则 Sat_{35} 会执行分组丢失操作。

如图 6 所示，当低轨卫星 Sat_{34} 收到消息后，执行上一步低轨卫星 Sat_{35} 相同的操作。不同的是，本文方案中认证消息传递不能经过相同的卫星，而低轨卫星 Sat_{34} 收到的消息来自 Sat_{35}，因此它不会将消息往回发送。

5.2 低轨星座组网群组密钥协商协议

如图 7 所示，在低轨星座组网中，消息在经过

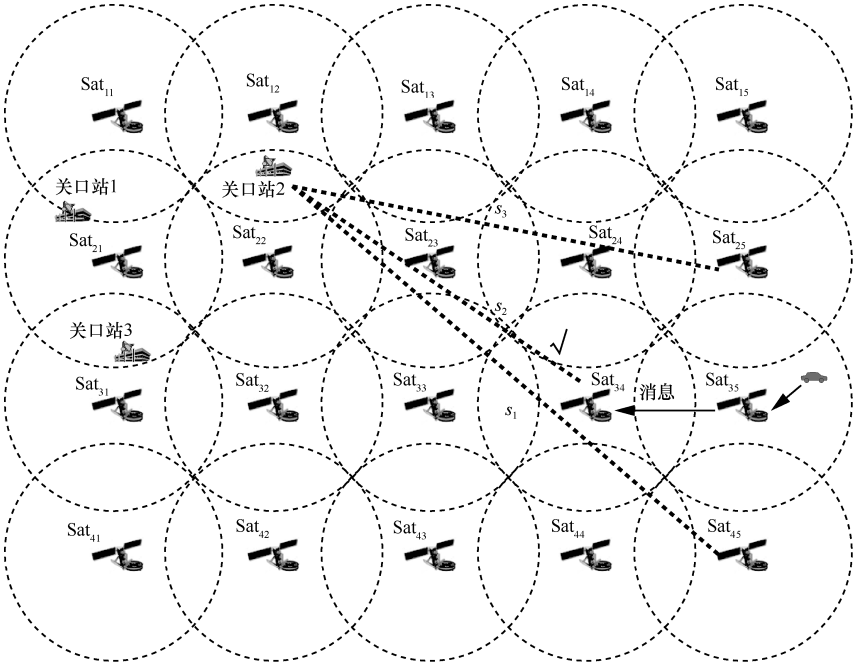


图 5 低轨卫星 Sat_{35} 路由选择情况

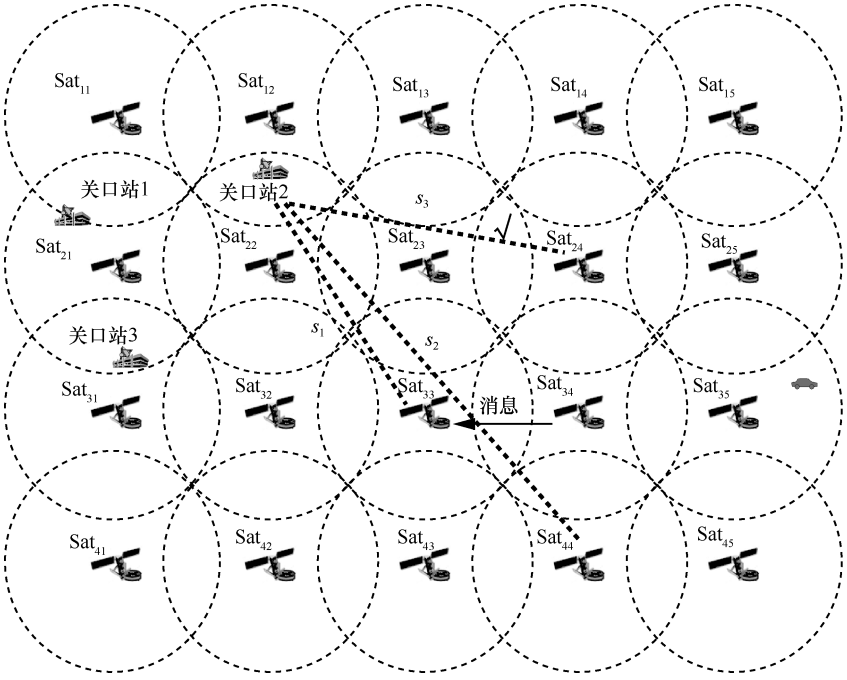


图 6 低轨卫星 Sat_{34} 路由选择情况

每一颗低轨卫星时都要使用相应的对称密钥进行一次解密和一次加密。这样，虽然保证了低轨星座组网的安全性，但是会影响消息在低轨星座组网中的传输效率。同时，每一颗卫星接收到消息之后都会进行一次解密操作和一次加密操作，容易遭受拒绝服务攻击。为了防止拒绝服务攻击的发生，同时保证传输过程的高效性，本文采用基于群组的密钥生成方法，同一轨道上的低轨卫星作为一个群组，相邻轨道上的低轨卫星作为一个群组，这样，将所有的低轨卫星划分成了多个群组，每个群组协商得到密钥之后会将密钥发送给低轨卫星关口站，这样，低轨卫星关口站会维护这些群组的密钥。通信的消息在群组内直接转发，当由一个群组进入另一个群组后，使用另外一个群组的密钥进行二次加密。这样，每个低轨卫星的运算强度是一样的，防止了拒绝服务攻击的发生。同时，传输的协议会在消息内容中附加消息经过的群组。这样，消息到达低轨卫星关口站的时候，由低轨卫星关口站根据消息经过的群组使用密钥依次解密。群组划分示意如图 8 所示。

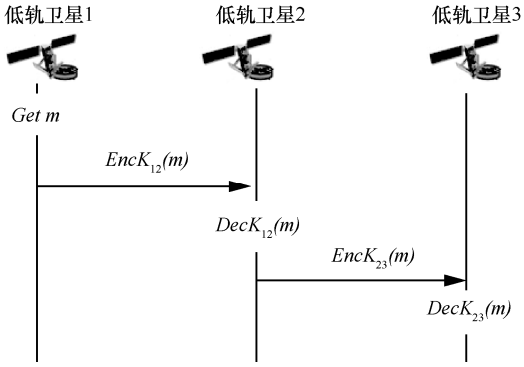


图 7　无群组密钥的低轨星座组网消息传输示意

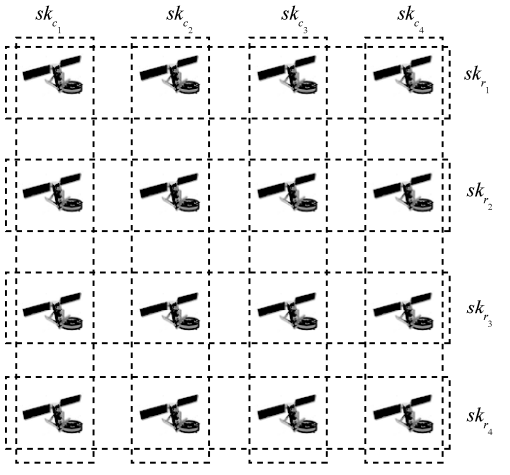


图 8　低轨卫星群组密钥协商示意

每个群组的密钥由这个群组内所有的对称密钥进行异或计算得到。以相邻轨道上的低轨卫星进行群组密钥协商为例，密钥协商过程如图 9 所示，具体算法如算法 3 所示。

算法 3　群组密钥协商算法

输入 lv_i, sk^g, ls_k

输出 sk^g

$Auth\_Result = Auth(lv_k, lv_i)$

if $Auth\_Result$=true then

　　计算　sk_{ik}

　　$sk^g = sk^g \oplus sk_{ik}$

end if

return　sk^g

当低轨卫星 1 进入预定轨道之后，此时只存在一颗低轨卫星，不需要进行群组密钥协商。当低轨卫星 2 进入预定轨道之后，与低轨卫星 1 进行认证并协商出对称密钥 sk_{12}。此时，群组密钥 $sk^g = sk_{12}$。

当低轨卫星 3 进入预定轨道之后，与低轨卫星 2 进行认证并协商出对称密钥 sk_{23}。此时，低轨卫星 2 使用群组密钥与 sk_{23} 进行异或运算得到新的对称密钥，即 $sk^g = sk_{12} \oplus sk_{23}$，并将新的群组密钥发送给组内其他成员。之后有新的低轨卫星加入群组时也是执行相同的操作。

6　安全性分析与性能分析

在低轨星座组网认证协议与消息传输过程中使用对称密钥来保证消息的私密性，协议可以抵抗仿冒等安全威胁。同时，协议中采用了伪随机数，保证了在星地传输时延较大的情况下能够防止重放攻击的发生。

在群组密钥协商协议中，由于低轨卫星之间都经过认证并建立了可靠的星间链路，在星间链路上广播群组密钥是安全的。同时，在群组密钥协商的过程中，卫星不需要知道群组中其他卫星的密钥，这样，单颗卫星被攻击之后其他卫星的密钥不会被泄露，只需要重新进行群组密钥协商即可。

为了对协议的性能进行测试，本文模拟了低轨星座组网的认证协议和群组密钥协商协议，经过多次实验分析其性能。实验在 3.1GHz Intel Core i5 的处理器上进行。实验中构建的低轨卫星星座有 6 个轨道，平均每个轨道上分布 10 颗卫星，共 60 颗卫

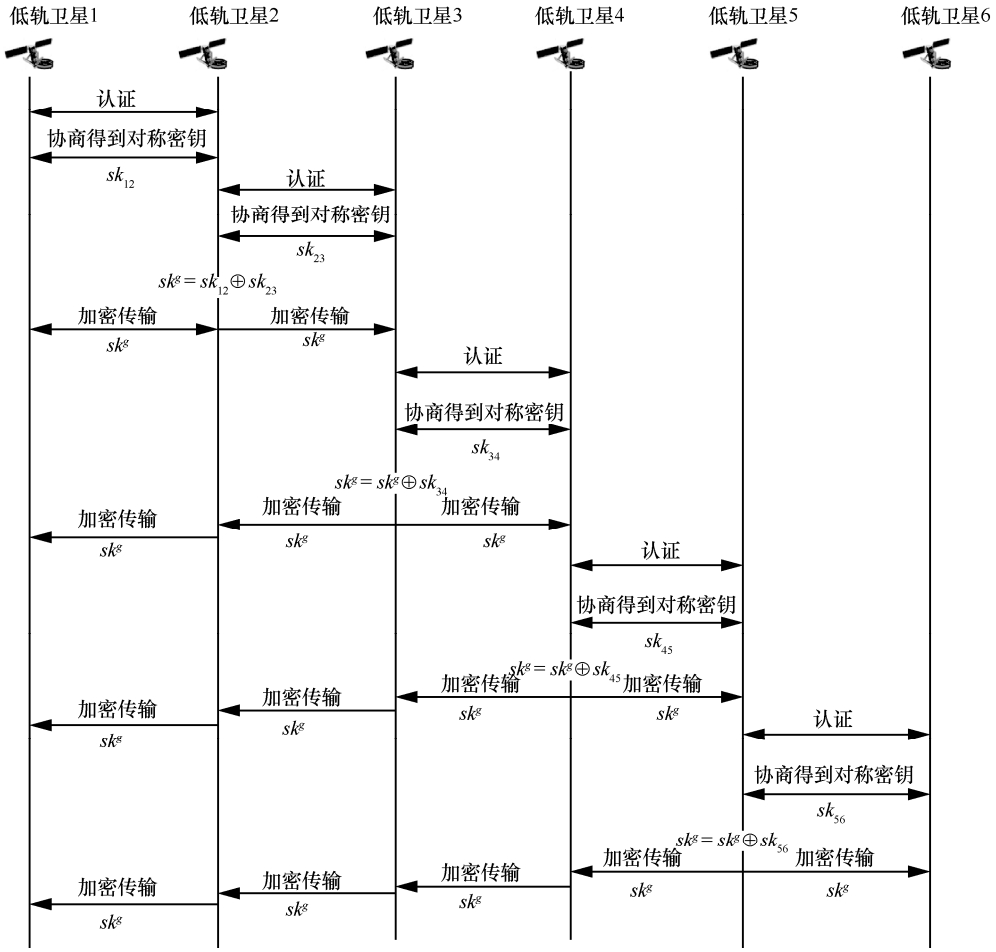


图 9　低轨卫星群组密钥协商协议流程

星，轨道倾角为 90°，轨道高度为 780 km。考虑星地传输存在通信时延，设定星地传输时延为 2.6 ms。

低轨星座组网认证协议的性能测试结果如图 10 所示。本文一共进行了 10 组实验来将本文方案与 3GPP AKA 协议做对比。从图 10 可以看出，本文方案认证时延最大为 10.30 ms，最小为 9.49 ms，平均时延为 9.80 ms。3GPP AKA 方案认证时延最大为 14.36 ms，最小为 9.41 ms，平均时延为 12.26 ms。本文方案比 3GPP AKA 方案效率提高了 20%的效率。

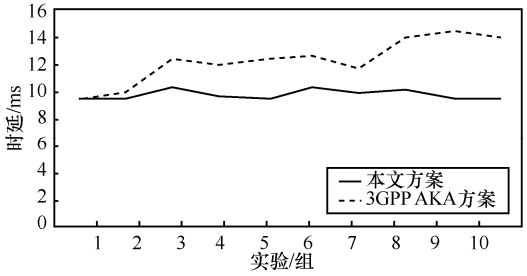


图 10　低轨星座组网认证协议的性能测试结果

实验还测试了不同加密位数对认证协议效率的影响，结果如图 11 所示。从实验结果可以看出，不同的加密位数对协议性能影响不大。

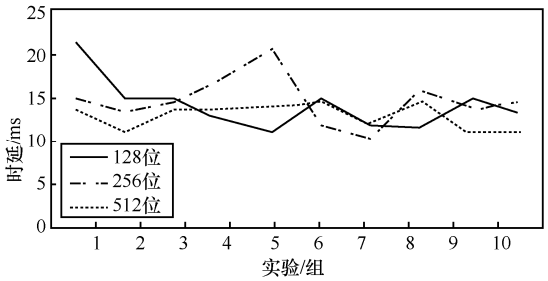


图 11　不同加密位数的低轨星座组网认证协议效率对比

低轨星座组网同轨道内群组密钥协商协议的性能测试结果如图 12 所示。实验从群组中只有一颗卫星的情况到群组中有 10 颗卫星的情况都进行了测试。低轨星座组网相邻轨道内群组密钥协商协议的性能测试结果如图 13 所示。实验从群组中只有一颗卫星的情况到群组中有 6 颗卫星的情况都进

行了测试。从图 13 可以看出随着群组中卫星数量的增多，群组密钥协商完成的时间也在增加。同轨道内群组密钥协商时延最高在 300 ms 左右，相邻轨道内群组密钥协商时延最高在 70 ms 左右。

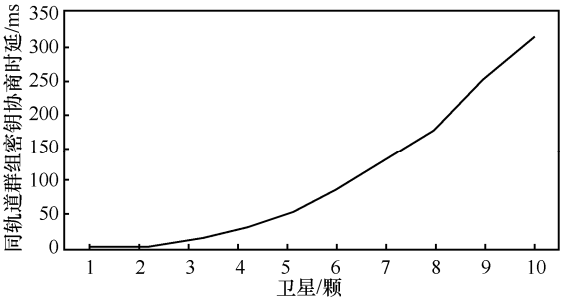


图 12　低轨星座组网同轨道内群组密钥协商协议的性能测试

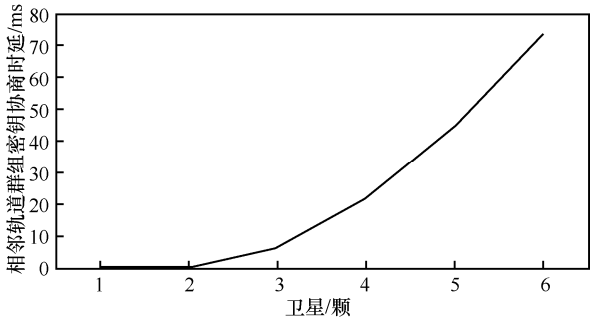


图 13　低轨星座组网相邻轨道内群组密钥协商协议的性能测试

除了考虑群组密钥协商协议的效率外，还要考虑采用该协议对整个传输效率的影响。低轨星座组网相邻轨道最大传输时延如图 14 所示，低轨星座组网同轨道最大传输时延如图 15 所示。实验结果表明，采用群组密钥协商协议比常规方案在传输时延上有所降低，但差距不明显，这是由于只考虑了一条消息的传递。

根据以上结果可知，低轨星座组网的认证协议比传统公钥协议效率有所提高，而且群组密钥协商协议能够在 300 ms 内协商完成，采用群组密钥协商协议的传输时延比常规方案的传输时延更小。

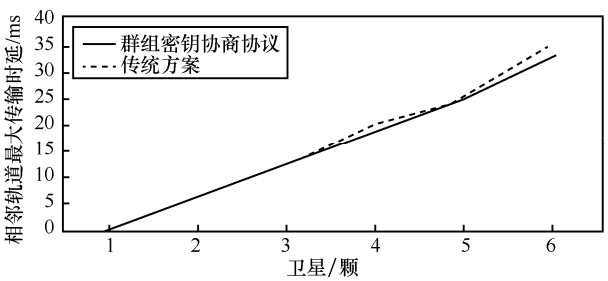


图 14　低轨星座组网相邻轨道最大传输时延

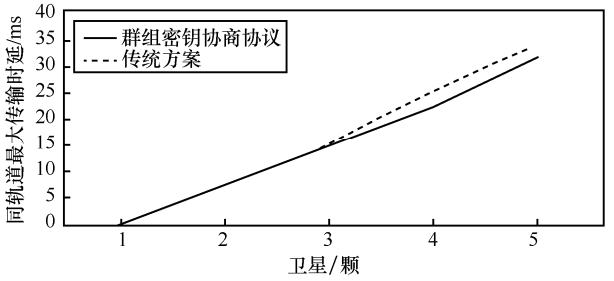


图 15　低轨星座组网同轨道最大传输时延

7　结束语

本文通过分析低轨星座组网的特点，设计了一种轻量级的低轨星座组网认证协议和群组密钥协商协议，并对协议进行了安全性分析和性能分析。本文提出的协议考虑了低轨卫星组网拓扑动态变化高、链路切换快的特点，设计的协议比 3GPP AKA 协议效率提高了 20%，同时，群组密钥协商时间约为 300 ms，采用群组密钥协商协议的传输时延比常规方案的传输时延更小。

在未来的研究中将完善本文设计的低轨星座组网以及群组密钥协商协议。低轨星座组网的认证还需要考虑更多的空间场景，包括太空环境对卫星通信的影响。同时，随着卫星技术的发展，可以在卫星上搭载更安全的公钥认证体系。

参考文献：

[1] 李凤华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11):156-168.
LI F H, YIN L H,WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications,2016, 37(11):156-168.

[2] 张小亮, 涂勇策, 马恒太,等. 一种适用于卫星通信网络的端到端认证协议[J]. 计算机研究与发展, 2013, 50(3):540-547.
ZHANG X L,TU Y C,MA H T, et al. An end-to-end authentication protocol for satellite communication network [J]. Journal of Computer Research and Development, 2013, 50(3):540-547.

[3] 徐志博, 马恒太. 一种用于卫星网络安全认证的协议设计与仿真[J]. 计算机工程与应用, 2007, 43(17):130-132.
XU Z B, MA H T. Design and simulation of security authentication protocol for satellite network [J]. Computer Engineering and Applications, 2007, 43(17):130-132.

[4] 徐日新, 陈小兵, 祝烈煌. CASTWED:卫星移动通信系统中一种结合可穿戴设备与智能终端的持续认证方案[J]. 通信学报, 2017, 38(8): 60-65.
XU R X, CHEN X B, ZHU L H. CASTWED: continuous authentication combining smart terminal with wearable devices in mobile satel-

lite communication system[J]. Journal on Communications, 2017, 38(8): 60-65

[5] 高婧, 黄望宗. 基于 ELGamal 数字签名的卫星网络认证方案[J].计算机工程与设计,2011,32(12):3980-3982，4029.
GAO J, HUANG W Z. Satellite network authentication scheme based on ELGamal digital signature[J]. Computer Engineering and Design, 2011, 32(12):3980-3982, 4029.

[6] CRUICKSHANK H S. A security system for satellite networks[C]// International Conference on Satellite Systems for Mobile Communications and Navigation. 1996:187-190.

[7] CHEN T H, LEE W B, CHEN H B. A self-verification authentication mechanism for mobile satellite communication systems[J]. Computers & Electrical Engineering, 2009, 35(1):41-48.

[8] 赖成喆, 郑东. 3GPP 认证和密钥协商协议综述[J]. 信息网络安全, 2016(8): 24-31.
LAI C Z, ZHENG D. Research on 3GPP authentication and key agreement protocols[J]. Information Network Security, 2016(8): 24-31.

[9] GAI K, QIU M. Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers[J]. IEEE Transactions on Industrial Informatics, 2018, PP(99):1.

[10] 陆峰, 郑康锋, 钮心忻, 等. 3GPP 认证与密钥协商协议安全性分析[J]. 软件学报, 2010, 21(7):1768-1782.
LU F, ZHENG K F, NIU X X, et al. Security analysis of 3GPP authentication and key agreement protocol [J]. Journal of Software, 2010, 21(7): 1768-1782.

[11] 周赤, 朱诗兵, 李长青. LTE 认证与密钥协商协议的安全分析及改进[J]. 现代电子技术, 2014(18):35-37.
ZHOU C, ZHU S B, LI C Q. Security analysis and improvement of LTE authentication and key agreement protocol [J]. Modern Electronics Technique, 2014(18):35-37.

[12] ZHANG M, FANG Y. Security analysis and enhancements of 3GPP authentication and key agreement protocol[J]. IEEE Transactions on Wireless Communications, 2005, 4(2):734-742.

[13] JUANG W S, WU J L. Efficient 3GPP authentication and key agreement with robust user privacy protection[C]// IEEE Wireless Communications and NETWORKING Conference. 2007: 2720-2725.

[14] LEE C C, CHEN C L, OU H H, et al. Extension of an efficient 3GPP authentication and key agreement protocol[J]. Wireless Personal Communications, 2013, 68(3): 861-872.

[15] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transaction on Information Theory, 1976, 22(22): 644-654.

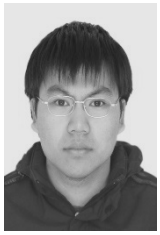
[16] JOUX A. A one round protocol for tripartite Diffie-Hellman[C]// International Algorithmic Number Theory Symposium. 2000:385-393.

[17] 陈虹, 徐嘉鸿, 肖振久. 基于身份的认证密钥协商协议的改进[J]. 计算机应用与软件, 2016(2):284-289.
CHEN H, XU J H, XIAO Z J, et al. Improvement of ID-based authenticated key agreement protocol[J]. Computer Applications and Software, 2016 (2): 284-289.

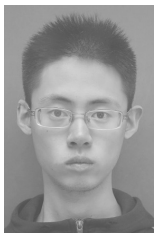
[18] 陈海红, 李军义. 新的基于身份认证的群密钥协商协议[J]. 计算机工程与应用, 2017, 53(21):103-109.
CHEN H H, LI J Y. Novel ID-based group authenticated key agreement scheme[J]. Computer Engineering and Applications, 2017, 53(21): 103-109.

[19] 3GPP. Technical specification group services and system aspects, 3G security, security architecture release 1999: TS 33.102 v 3.13.0[S]. 2002

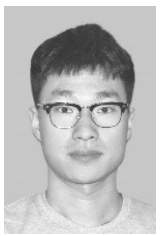
[作者简介]



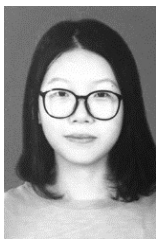
张子剑（1983-），男，北京人，博士，北京理工大学副教授、硕士生导师，主要研究方向为密码协议设计与安全性分析、隐私保护、智能电网、支付安全。



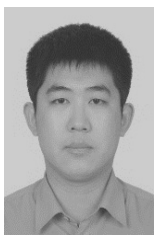
周琪（1995-），男，湖南怀化人，北京理工大学硕士生，主要研究方向为天地一体化网络安全、移动互联网安全等。



张川（1991-），男，河北邯郸人，北京理工大学博士生，主要研究方向为天地一体化网络安全、物联网安全、云计算安全。



童逍瑶（1997-），女，浙江绍兴人，主要研究方向为信息安全。



李春磊（1986-），男，北京人，中国民航信息集团公司工程师，主要研究方向为卫星通信、大数据、数据中心。

王龙（1988-），男，河北衡水人，北京理工大学硕士生，主要研究方向为天地一体化网络安全、移动互联网安全等。