适用于双层卫星网络的星间组网认证方案

朱辉[1,2]，武衡[1]，赵海强[2]，赵玉清[1]，李晖[1]
（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；
2. 通信网信息传输与分发技术重点实验室，河北 石家庄 050081）

摘 要：为解决双层卫星网络高、低轨卫星间的组网认证问题，提出了一种安全、高效的星间组网认证方案。该方案基于对称加密设计，能够在无可信第三方参与的情况下，实现高、低轨卫星间的信任建立和安全通信。针对卫星网络时钟高度统一、节点运行轨迹可预测的场景特点，设计了认证预计算机制，有效提升了星间组网的认证效率。形式化证明与安全性分析表明，所提方案能够满足卫星在组网阶段的多种安全需求。性能分析及仿真结果显示，所提方案具有较低的计算和通信开销，能够实现卫星在资源有限场景下的安全组网认证。

关键词：双层卫星网络；星间组网认证；对称加密；安全协议
中图分类号：TP302
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019058

Efficient authentication scheme for double-layer satellite network

ZHU Hui[1,2], WU Heng[1], ZHAO Haiqiang[2], ZHAO Yuqing[1], LI Hui[1]
1. School of Cyber Engineering, Xidian University, Xi'an 710071, China
2.Science and Technology on Communication Networks Laboratory, Shijiazhuang 050081, China

Abstract: To solve the issue of networking authentication among GEO and LEO satellites in double-layer satellite network, a secure and efficient authenticated key agreement scheme was proposed. Based on symmetric encryption, the proposed scheme can achieve trust establishment and secure communication between satellites without the trusted third party. Meanwhile, considering characteristics of highly unified clock and predictable satellite trajectory in satellite networks, a pre-calculation method was designed, which can effectively improve the authentication efficiency of satellite networking. Moreover, formal proof and security analysis demonstrate that the scheme can satisfy various security requirements during satellite networking. Performance analysis and simulation results show that the scheme has low computation and communication overhead, which can achieve the authentication of satellite networking in resource-limited scenarios.

Key words: double-layer satellite network, satellite networking authentication, symmetric encryption, secure protocol

1 引言

利用卫星通信网弥补 5G 基站的覆盖盲区，解决山区、极地、远洋等地区的高带宽通信难题，已经成为学术和工业领域的一个重要研究方向。包含高轨卫星（GEO，geostationary earth orbit）和低轨卫星（LEO，low earth orbit）的双层卫星网络（如图 1 所示），由于能够提供“全球覆盖、随遇接入”的通信服务，一提出就受到业内的广泛关注[1]。

收稿日期：2018−03−16；**修回日期**：2019−01−24
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800300）；国家自然科学基金资助项目（No.61672411, No.U1401251）；通信网信息传输与分发技术重点实验室开放课题基金资助项目（No.KX172600023）；高等学校学科创新引智计划基金资助项目（No.B16037）
Foundation Items: The National Key Research and Development Program of China (No.2016YFB0800300), The National Natural Science Foundation of China (No.61672411, No.U1401251), Science and Technology on Communication Networks Laboratory (No.KX172600023), China's 111 Project (No.B16037)

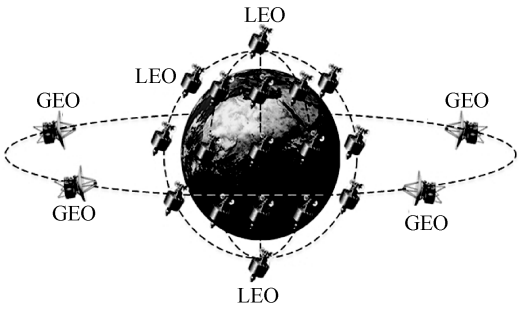

图 1 双层卫星网络模型

然而，卫星网络的组网运行面临严峻的安全挑战[2]。一方面，由于双层卫星网络涉及上百颗不同轨道的卫星，无法维持稳定的拓扑结构，频繁的链路切换显著增加了该网络遭受入侵的可能；另一方面，星间通信采用开放链路，通信内容易被监听、篡改和伪造，使卫星网络的组网过程极有可能因遭受恶意干扰而无法完成。因此，卫星网络的安全、快速组网是确保其稳定工作的前提。

身份认证是保障卫星网络安全运行的一项重要技术。然而，双层卫星网络特殊的部署环境，对星间身份认证协议的设计提出了更高的要求。首先，星上资源有限，难以应对较大的计算开销；其次，星间距离较远，通信时延长达数百毫秒，这种时延不可忽略[3]；最后，由于双层卫星网络包含卫星数量众多，认证协议需要尽量减少地面站等第三方的参与，确保卫星组网的自主性和独立性。

针对卫星网络的安全组网问题，研究们者提出了一系列身份认证方案。基于公钥（或证书）的方案具有密钥管理简单、不需要地面频繁参与的优势，然而，此类方案认证时需要进行证书传递和复杂的公钥、私钥计算，存在通信和计算开销较大等问题。基于对称加密的方案计算开销较少，但是通常认证过程繁琐，或者需要可信第三方的参与，需要进行优化改进才能应用于卫星网络。此外，现有的许多方案由于并非针对双层卫星网络设计，在使用上存在一定的不合理性。

针对上述问题，本文综合考虑双层卫星网络时钟高度统一、节点运行轨迹可预测的场景特点，基于对称加密，提出了一种安全、高效的认证与密钥协商方案（GL-AKA，GEO and LEO authenticated key agreement）。该方案能够在无可信第三方参与的情况下，实现 GEO 和 LEO 之间的信任建立和安全通信。分析表明，本方案能够有效抵御常见的各类攻击，且具有较低的计算和通信开销。

2 相关工作

与卫星网络相关的安全研究一直是学术界的研究热点，其中，身份认证技术由于能够保证卫星网络的安全组网，受到了学术界的广泛关注。Liu 等[4]分析了身份认证对于卫星组网的重要意义，研究了该场景下的诸多安全威胁，如窃听、会话劫持、非授权访问等。Chowdhury 等[5]基于卫星节点资源有限的场景特点，为多网融合的卫星系统提出了一个认证框架。

针对卫星网络的身份认证方案主要分为 2 类。一部分研究者主张采用公钥、证书等技术。任方等[6]提出了一种基于证书的公钥基础设施，采用分布式证书颁发机构，能够在复杂多变的卫星网络中实现星间身份认证。Zhong 等[7]利用基于身份的公钥体制设计了一种适用于卫星网络的星间认证与密钥协商方案。然而，基于公钥的认证方案由于计算开销较大，在应用上存在一定的局限性。

另一部分研究者倾向于采用对称加密进行方案设计。Zhang 等[8]基于对称加密提出了一种认证和密钥协商方案，并通过形式化分析证明了其安全性。然而，Qi 等[9]经过分析发现该方案存在一些不足，如面对拒绝服务攻击的不安全性、存在密钥更新问题等，对此，Qi 提出了一种增强型认证方案。但是，许多基于对称密钥的方案依旧存在认证过程复杂、需要可信第三方参与等问题。

鉴于资源有限的星上环境，对认证方案的轻量化改进也是一个重要的研究方向。Vossaert 等[10]使用对称加密设计了一种适用于资源有限节点的轻量化认证方案，性能分析表明该方案能够有效地减少卫星在认证过程中的计算开销。Lee 等[11]为进一步减少星间认证的计算开销，提出了一种仅使用散列函数和异或计算的认证方案，该方案的计算开销极低。然而，Zhang 等[12]发现该方案因过多的简化，无法保证星间认证的安全性，易受到拒绝服务攻击、重放攻击等多种安全威胁，故对该方案进行改进，提高了安全性。

卫星的身份匿名性也是设计认证方案时的一个关注重点。为了防止卫星身份信息的泄露，Tsai[13]提出了一种匿名认证方案，该方案在用户身份匿名保护上有了较大的改进，能够有效地防止卫星节点真实身份信息的泄露。然而，匿名保护算法也在一定程度上增加了认证方案的计算复杂度。为

了提升认证效率，Yoon 等[14]在认证方案中使用了一种轻量化的匿名技术，实现匿名保护的同时有效地减少了匿名运算带来的额外开销。

综上所述，现有认证方案在安全性、轻量化等方面进行了较大改进。但是，上述方案并非针对双层卫星网络设计，在应用上还存在局限性。本文旨在针对双层卫星网络，基于对称加密技术，提出一种安全、高效的组网认证方案。

3　预备知识

3.1　系统模型

高、低轨卫星间的组网认证主要考虑 GEO 和 LEO。其中，GEO 使用地球同步轨道，由于星间位置相对固定，多颗 GEO 能够组成一个结构稳定的卫星网络； LEO 使用极地轨道，由于运行速度较快、公转周期较短，通信链路无法长时间维持。受轨道设置的影响，LEO 和 GEO 网络之间难以维持稳定的拓扑结构。在运行过程中，为保证与 GEO 网络通信的稳定性，LEO 需要在 GEO 网络的不同接入点之间进行频繁的链路切换。

如图 2 所示，在 2 个 GEO 与一个 LEO 组成的最小双层卫星网络系统中，可以看出，LEO 与 GEO 之间的链路切换主要发生在极点附近。当顺时针运行的 LEO 经过北极点时，由于地球的阻挡，其与 GEO_1 之间的通信链路会出现中断。此时，该 LEO 需要与 GEO_2 建立新的通信链路才可以再次接入 GEO 网络。

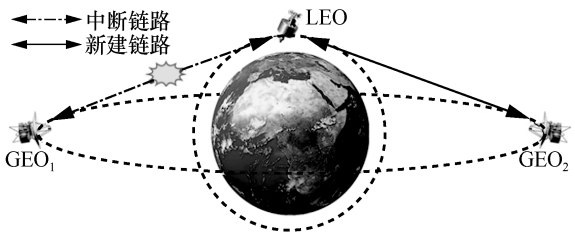

图 2　星间链路切换示意

由于 GEO 在极点附近存在覆盖盲区，经过极点时，LEO 会暂时脱离 GEO 网络。为保证卫星网络的运行安全，每次链路切换时，卫星之间都需要重新进行身份认证并协商新的会话密钥，为保证卫星通信的连续性，该过程需要在保证安全的前提下尽量减少切换时延。

3.2　攻击者模型

星间通信链路高度开放，攻击者能够通过信道监听、信令重放等方式对星间组网认证实施干扰。这一场景特点与安全协议形式化分析中常用到的 Dolev-Yao 模型[15]所定义的“网络处于攻击者的控制之下”具有一致性，因此，本文认为该场景下的攻击者也具有与 Dolev-Yao 模型中的攻击者相似的网络攻击能力，对攻击者的具体定义如下。

1) 攻击者能够监听、拦截和存储卫星间的全部会话，包括所有的认证信令。

2) 攻击者能够通过构造的代理节点与目标卫星建立连接并参与星间组网认证。

3) 攻击者能够对存储的会话内容进行破解，得到诸如会话密钥、认证密钥等关键参数。

4) 攻击者能够重放拦截的认证信令或利用破解得到的关键参数伪造认证信令。

根据文献[4]对卫星网络安全威胁的研究，攻击者对卫星网络发起的攻击主要包括以下 2 类。

1) 实体假冒。攻击者通过分析星间认证信令，推断认证流程，进而构造卫星代理节点，通过重放、伪造认证信令等方式，实施网络入侵。

2) 拒绝服务攻击。攻击者通过搜集认证节点的身份信息，利用得到的合法身份信息伪造认证信令，向目标卫星频繁发送认证请求，不断消耗卫星的计算资源和通信带宽，达到瘫痪卫星的目的。

3.3　安全需求

卫星通信网涉及地面上亿用户的通信安全，需要极高的安全性。为保证卫星间的组网安全，认证协议需要满足以下安全需求。

1) 双向认证。为了保证星间组网的安全性，认证方案需要保证协议双方均能够检验对方身份的合法性。

2) 抵御重放攻击。认证方案需要设计有效的抗重放机制，防止攻击者通过重放拦截的星间认证信令，实施网络攻击。

3) 抵御拒绝服务攻击。由于卫星资源有限，难以应对大量接入请求，认证方案需要能够对合法用户进行快速区分。

4) 前向安全性和后向安全性。由于攻击者极有可能破解拦截到的星间会话，认证方案必须保证星间通信在安全方面的前向/后向独立性。

3.4　BAN 逻辑

BAN 逻辑最初由 Burrows、Abaci 和 Neecham 联合提出，目前，已广泛用于认证协议安全性的形式化分析[16]。表 1 列举了使用 BAN 逻辑时用到的

基本符号及其含义。相关 BAN 逻辑规则描述如下。

1) 消息含义规则 $\dfrac{P|\equiv P\xleftrightarrow{K}Q, P\lhd\{X\}_K}{P|\equiv Q|\sim X}$

2) 新鲜性验证规则 $\dfrac{P|\equiv\#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

3) 控制规则 $\dfrac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$

4) 消息接收规则

① $\dfrac{P\lhd(X,Y)}{P\lhd X}$

② $\dfrac{P|\equiv P\xleftrightarrow{K}Q, P\lhd\{X\}_K}{P\lhd X}$

5) 新鲜性规则 $\dfrac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$

6) 信念规则

① $\dfrac{P|\equiv X, P|\equiv Y}{P|\equiv(X,Y)}$

② $\dfrac{P|\equiv(X,Y)}{P|\equiv X}$

③ $\dfrac{P|\equiv Q|\equiv(X,Y)}{P|\equiv Q|\equiv X}$

④ $\dfrac{P|\equiv Q|\sim(X,Y)}{P|\equiv Q|\sim X}$

表 1 BAN 逻辑符号及其含义

符号	含义
P,Q	通信主体
X,Y	消息语句
$Q\xleftrightarrow{K}P$	P 和 Q 之间的共享密钥 K
(X,Y)	消息的连接
$P\|\equiv X$	P 相信消息 X
$P\lhd X$	P 收到了消息 X
$P\|\sim X$	P 发送了消息 X
$P\|\Rightarrow X$	P 对消息 X 具有控制权
$\#(X)$	消息 X 是新鲜的
$\{X\}_K$	用密钥 K 加密 X 得到的密文

4 GL-AKA 星间组网认证方案

针对双层卫星网络的场景特点，为满足星间组网的安全需求，本节提出了一种适用于高、低轨卫星的星间组网认证方案，包括系统初始化、认证信息注册、认证预计算和星间切换认证这 4 个部分。表 2 列举了 GL-AKA 中使用的符号及其含义。

表 2 GL-AKA 使用的符号及其含义

符号	含义
IDKey	身份信息匿名保护密钥
MainKey	星间认证的主密钥
AuthKey	星间认证的认证密钥
f_{TID}	临时身份生成函数
f_{AK}	认证密钥生成函数
f_{TK}	时间戳保护序列生成函数
f_{MAC}	消息验证码生成函数
T_0	当前时间
T_{TID}	用于生成临时身份的时间戳
T_{Auth}	用于生成认证密钥的时间戳
T_{AV}	用于生成认证向量的时间戳
RID	卫星的真实身份
TID	卫星的临时身份
RAND	一次性随机数
TK	时间戳保护序列
MAC	消息验证码
AV	认证向量
RES	认证响应值
CK	会话密钥

4.1 系统初始化

系统初始化由地面站在卫星发射准备阶段进行，主要包括认证信息的生成和分发，如 ID、IDKey、MainKey 等，其中，1) ID 是卫星的身份信息，用于对卫星节点进行唯一标识；2) IDKey 是卫星身份信息的匿名保护密钥，属于 GEO 与 LEO 群组之间的共享秘密，用于认证阶段 LEO 临时身份的生成；3) MainKey 是星间认证的主密钥，属于 GEO 和 LEO 卫星之间的共享秘密，用于生成认证密钥 AuthKey。

4.2 认证信息注册

认证信息注册包括 2 个步骤，分别是 LEO 首次接入 GEO 网络时的身份认证和随后的信息注册。卫星间的首次信任建立需要进行一次完整的身份认证，如图 3 所示。该过程包括以下 4 个步骤。

步骤 1 LEO 对真实身份 RID 进行匿名处理。首先，LEO 通过星载时钟获取时间戳 T_{TID}，然后，基于获取的 T_{TID} 和预置的 IDKey，LEO 计算本次认证应使用的 TID。

$$\text{TID}=f_{\text{TID}}\left(\text{IDKey},T_{\text{TID}}\|\text{RID}\right)$$

计算完成后，LEO 将 TID 连同认证请求一并发

送给 GEO。

步骤 2　收到认证请求后，GEO 首先对该请求的合法性进行验证，如 1)所示。

1) GEO 使用预置的 IDKey 对 TID 解密。如果得到的 T_{TID} 满足 $T_{\mathrm{TID}}-T_0<\Delta T_{\mathrm{TID}}$，且 RID 命名合法，则完成验证，继续执行后续步骤；否则终止认证，释放连接。

对认证请求的验证通过后，GEO 向 LEO 返回一个 AV，其生成过程如 2)~4)所示。

2) GEO 通过星载时钟获取时间戳 T_{Auth}。基于获取的 T_{Auth} 和预置的 MainKey，GEO 计算本次认证应使用的 AuthKey。

$$\mathrm{AuthKey}=f_{\mathrm{AK}}\left(\mathrm{MainKey},T_{\mathrm{Auth}}\right)$$

3) GEO 生成一个一次性随机数 RAND。基于生成的 RAND 和 AuthKey，GEO 计算时间戳保护序列 TK。

$$\mathrm{TK}=f_{\mathrm{TK}}\left(\mathrm{AuthKey},\mathrm{RAND}\right)$$

4) GEO 通过星载时钟获取时间戳 T_{AV}。基于生成的 RAND、获取的 T_{AV}、存储的 SGID（GEO 的群组身份标识），GEO 计算该 AV 对应的消息验证码 MAC。

$$\mathrm{MAC}=f_{\mathrm{MAC}}\left(\mathrm{AuthKey},\mathrm{RAND}\|T_{\mathrm{AV}}\|\mathrm{SGID}\right)$$

随后，GEO 将 RAND、T_{AV}、TK、SGID、MAC 合并成 AV。

$$\mathrm{AV}=\mathrm{RAND}\|T_{\mathrm{AV}}\oplus\mathrm{TK}\|\mathrm{SGID}\|\mathrm{MAC}$$

5) GEO 计算该 AV 对应的会话密钥 CK 和预期响应 XRES。

$$\mathrm{CK}=f_{\mathrm{CK}}\left(\mathrm{AuthKey},\mathrm{RAND}\right)$$

$$\mathrm{XRES}=f_{\mathrm{RES}}\left(\mathrm{CK},\mathrm{RAND}\right)$$

计算完成后，GEO 存储 CK 和 XRES，并将 AV 返回给 LEO。

步骤 3　收到 AV 后，LEO 利用同样的方法生成 AuthKey，并对收到的 AV 进行解析，具体过程如下。

1) LEO 利用生成的 AuthKey 和 AV 中的 RAND 计算 TK。使用 TK 恢复出 AV 中的 T_{AV} 后，判断 $T_{\mathrm{AV}}-T_0<\Delta T_{\mathrm{AV}}$ 是否成立。如果满足，继续执行后续步骤；否则，终止认证。

2) LEO 利用生成的 AuthKey 和 AV 中的 RAND、T_{AV} 和 SGID，采用相同的方式计算 XMAC。如果本地计算得到的 XMAC 与 AV 中的 MAC 相等，完成对 GEO 的认证；否则，认证失败。

认证成功后，LEO 利用 RAND 和 AuthKey 计算出 CK 和 RES，并将 RES 返回给 GEO。

步骤 4　收到 RES 后，GEO 比较收到的 RES 和存储的 XRES 是否相等。如果相等，完成对 LEO 的认证；否则，认证失败。

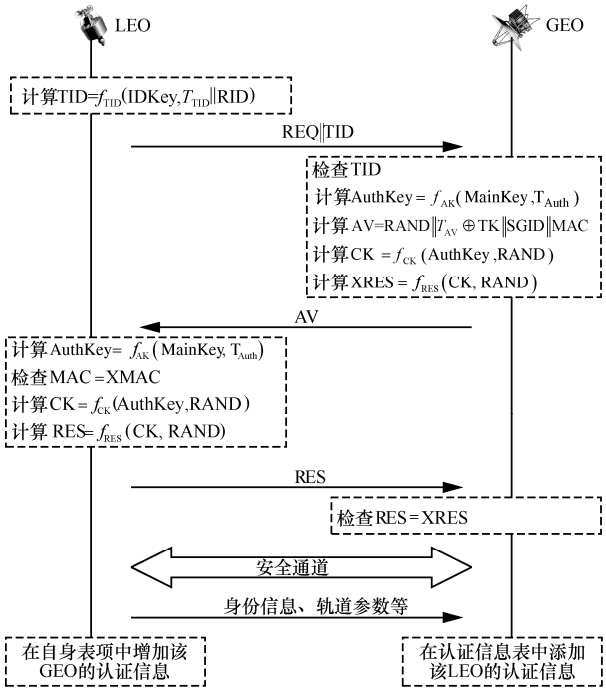

图 3　认证信息注册过程

认证完成后，LEO 在 GEO 的认证信息表中注册认证信息，包括自身 ID、轨道参数等必要信息；并在自身维护的表项中增加该 GEO 的认证信息。信息注册完成后，认证双方即可在各自存储的认证信息表的协助下预计算下次组网认证所需要的认证参数。

4.3　认证预计算

为减少卫星在认证阶段的计算开销，本文方案基于卫星的时钟同步性和轨位可预测性设计了认证预计算机制，该过程由 GEO 和 LEO 独立完成，具体如下。

1) Pre-LEO。LEO 需要预计算的认证参数有 TID 和 RES。LEO 首先通过轨位预测技术计算与目标 GEO 的认证时间点，得到 T_{TID}、T_{Auth}、T_{AV} 这 3 个参数。接下来，LEO 分别通过 T_{TID} 和 T_{Auth} 生成下次认证时应该使用的 TID 和 AuthKey。随后，LEO 使用上次认证时 AV 中的 RAND 和新生成的 AuthKey 计算 RES。计算完毕后，LEO 在认证信息表中存储预计算得到的 TID 与 RES。

2) Pre-GEO。GEO 需要预计算的认证参数有 XTID、XRES、AV 和 CK。同样，GEO 首先通过轨位预测技术计算与目标 LEO 的认证时间点，得到 T_{TID}、T_{Auth}、T_{AV} 这 3 个参数。接下来，GEO 采用和 Pre-LEO 相同的方法计算 XTID、AuthKey 和 XRES。最后，GEO 生成一个 RAND 并基于该 RAND 计算 AV 和 CK。计算完毕后，GEO 在认证信息表中存储 XTID、XRES、AV、CK。

预计算完成之后，LEO 和 GEO 的认证信息表中分别存储下次认证所需各项参数，再次进行组网认证时，卫星只需要通过查表就可以得到所需要的认证参数。

4.4 星间切换认证

当 LEO 再次与已经注册过认证信息的 GEO 进行认证时，只需要执行轻量化的认证协议，具体步骤如下。

步骤 1 LEO 首先判断自身轨道参数是否发生改变。如果出现轨道摄动，由于预计算参数已经失效，需要按照 4.2 节所述的认证过程重新进行身份认证，并更新认证信息；如果轨道参数正常，LEO 将预计算得到的 TID 和 RES 连同认证请求一起发送给 GEO。

步骤 2 收到认证请求后，GEO 将收到的 TID、RES 与存储的 XTID、XRES 进行比较。如果相等，完成对该 LEO 认证，返回预计算得到的 AV；如果不相等，重新执行 4.2 节所述认证过程。

步骤 3 收到 AV 后，LEO 首先验证该 AV 的新鲜性，如果满足新鲜性要求，继续验证该 AV 中的 MAC 与计算得到的 XMAC 是否相等。如果相等，完成认证，并可使用该 AV 对应的 CK 与 GEO 进行安全通信；如果不相等，认证失败。

5 方案分析

5.1 基于 BAN 逻辑的安全性证明

由于信息注册阶段的认证过程和切换认证阶段的认证过程结构基本相同，本节主要对认证过程较为复杂的前者进行安全性证明。下文中，A、B 分别为 LEO 和 GEO 的 ID。

1) 协议理想化

本阶段卫星间所传递消息的理想化模型如下。

消息 1 TID：$\{\mathrm{ID-A},T_{\mathrm{TID}}\}_{K_{\mathrm{ID}}}$

消息 2 AV：$(\mathrm{RAND},T_{\mathrm{AV}}\oplus\mathrm{TK},\{\mathrm{RAND},T_{\mathrm{AV}}\}_{K_{\mathrm{AB}}})$

消息 3 RES：$\{\mathrm{RAND}\}_{\mathrm{CK}}$

2) 协议目标

目标 1 $\mathrm{A}\mid\equiv\mathrm{RAND}$

目标 2 $\mathrm{A}\mid\equiv\mathrm{B}\mid\equiv\mathrm{RAND}$

目标 3 $\mathrm{B}\mid\equiv\mathrm{A}\mid\equiv\mathrm{RAND}$

3) 初始假设

本协议的初始化假设如下。

假设 1 $\mathrm{B}\mid\equiv\mathrm{A}\overset{K_{\mathrm{ID}}}{\longleftrightarrow}\mathrm{B}$

假设 2 $\mathrm{A}\mid\equiv\mathrm{A}\overset{K_{\mathrm{AB}}}{\longleftrightarrow}\mathrm{B}$

假设 3 $\mathrm{B}\mid\equiv\mathrm{A}\overset{\mathrm{CK}}{\longleftrightarrow}\mathrm{B}$

假设 4 $\mathrm{A}\mid\equiv\ \mathrm{B}\mid\Rightarrow\mathrm{RAND}$

假设 5 $\mathrm{A}\mid\equiv\#(T_{\mathrm{TID}})$

假设 6 $\mathrm{A}\mid\equiv\#(T_{\mathrm{AV}})$

假设 7 $\mathrm{B}\mid\equiv\#(\{\mathrm{RAND}\}_{\mathrm{CK}})$

4) 协议分析

本协议的部分安全性证明如下。

由消息 1 可得

① $\mathrm{B}\lhd\{\mathrm{ID-A},T_{\mathrm{TID}}\}_{K_{\mathrm{ID}}}$

由语句①和假设 1，根据消息含义规则得

② $\mathrm{B}\mid\equiv\mathrm{A}\mid\sim(\mathrm{ID-A},T_{\mathrm{TID}})$

由语句②和假设 5，根据新鲜性规则得

③ $\mathrm{B}\mid\equiv\#(\mathrm{ID-A},T_{\mathrm{TID}})$

此时，B 相信 LEO 群组中有一颗 ID 为 A 的卫星发来了认证请求，并且该消息不是重放消息。

由消息 2 可得

④ $\mathrm{A}\lhd(\mathrm{RAND},T_{\mathrm{AV}}\oplus\mathrm{TK},\{\mathrm{RAND},T_{\mathrm{AV}}\}_{K_{\mathrm{AB}}})$

由语句④，根据消息接收规则可得

⑤ $\mathrm{A}\lhd\{\mathrm{RAND},T_{\mathrm{AV}}\}_{K_{\mathrm{AB}}}$

由语句⑤和假设 2，根据消息含义规则可得

⑥ $\mathrm{A}\mid\equiv\mathrm{B}\mid\sim(\mathrm{RAND},T_{\mathrm{AV}})$

由语句⑥和假设 6，根据新鲜性规则可得

⑦ $\mathrm{A}\mid\equiv\#(\mathrm{RAND},T_{\mathrm{AV}})$

此时，A 相信收到的消息确实来自 B，并且不是重放消息，完成了对 B 的认证。

由语句⑥和语句⑦，根据新鲜性验证规则和信念规则可得

⑧ $\mathrm{A}\mid\equiv\mathrm{B}\mid\equiv\mathrm{RAND}$

由语句⑧和假设 7，根据控制规则得

⑨ $\mathrm{A}\mid\equiv\mathrm{RAND}$

由消息 3 可得

⑩ $\mathrm{B}\lhd\{\mathrm{RAND}\}_{\mathrm{CK}}$

由语句⑩和假设 3，根据消息含义规则得

⑪ $\mathrm{B}\mid\equiv\mathrm{A}\mid\sim\mathrm{RAND}$

此时，B 相信收到的消息确实来自 A，并且不是重放消息，完成了对 A 的认证。

由语句⑪，根据新鲜性验证规则可得

⑫ $B|\equiv A|\equiv RAND$

由语句⑧、⑨、⑫得，A、B 均认可 RAND 的有效性，并同意使用由该 RAND 和 AuthKey 衍生而来的会话密钥 CK 进行通信。

5.2 安全性分析

5.2.1 双向认证

本文所提方案能够实现 GEO 和 LEO 之间的双向认证。进行身份认证时，LEO 通过判断由本地计算得到的 XMAC 与 AV 中的 MAC 是否相等实现对 GEO 的身份认证；GEO 通过判断本地存储的 XRES 与返回的 RES 是否相等实现对 LEO 的身份认证。

对于 MAC 和 RES，其计算需要 AuthKey。如果不具有有效的 AuthKey，GEO 无法生成包含正确 MAC 的 AV，LEO 也无法返回正确的 RES。同时，考虑到 AuthKey 由 MainKey 基于时间生成，存在有效期，因此攻击者无法重复使用已破解的 AuthKey。而对于 MainKey，由于该参数由地面站在发射阶段写入卫星，不在会话中传递，故不存在泄露风险。

5.2.2 抵御重放攻击

本文所提方案能够有效抵御攻击者的重放攻击。由于卫星网络具有时钟高度同步的特点，可以采用时间戳技术抵御重放攻击。

进行接入认证时，GEO 和 LEO 之间需要传递的认证参数有 TID、AV 和 RES。其中，TID 的生成需要时间戳 T_{TID}，GEO 能够借此判断 TID 的新鲜性；AV 中包含有加密后的时间参数 T_{AV}，LEO 能够结合 MAC 值判断收到的 AV 是否为重放消息；RES 和 AV 存在对应关系，攻击者无法通过重放过期的 RES 欺骗 GEO。

5.2.3 抵御拒绝服务攻击

本文所提方案能够有效地抵御攻击者的拒绝服务攻击。对于卫星网络，攻击者可以通过向目标卫星频繁发送接入请求来消耗其有限的计算资源。本文方案通过临时身份对接入请求的合法性进行鉴别，缓解了卫星在认证阶段的计算压力。

进行接入认证时，LEO 发送的认证请求需要包含 TID。GEO 能够通过解密 TID 判断该接入请求的合法性，避免了后续的无效计算。同时，本方案针对卫星轨位可预测的特性，设计了认证预计算机制。GEO 除首次认证需要进行即时计算外，只需要通过查表和比较就可以完成星间身份认证，有效地减少了认证过程中的计算开销。

5.2.4 前向安全性与后向安全性

本文所提方案能够有效保证星间身份认证的前向安全性和后向安全性。

每次切换认证完成后，卫星间都会使用新协商的会话密钥 CK 进行通信。因此，即使攻击者得到了部分 CK，也无法解密卫星间的所有通信内容。同时，由于 CK 的生成主要基于 AuthKey 和 AV 中的 RAND，攻击者也无法通过破译得到的 AuthKey 继续生成新的 CK，保证了星间会话的独立性。

5.2.5 身份匿名性

本文所提方案能够有效地避免卫星身份信息的泄露。进行接入认证时，LEO 使用 TID 发出认证请求。由于不具有有效 IDKey，攻击者无法通过截获的 TID 获取卫星的真实身份信息，保证了节点身份的匿名性。

表 3 列举了本文方案与同类无线方案在安全性上的对比结果。通过分析可以发现，本方案在保证星间认证安全的基础上，还对卫星进行身份信息匿名化处理。同时，本文方案利用卫星网络的时钟同步优势，避免了认证过程产生的同步开销。

表 3　本方案与现有方案在安全性上的对比

方案	双向认证	重放攻击	DOS 攻击	前向/后向安全性	匿名保护	同步开销
本文方案	✓	✓	✓	✓	✓	×
文献[17]方案	✓	✓	✓	✓	✓	✓
文献[18]方案	✓	✓	✓	✓	×	×
文献[19]方案	✓	✓	✓	✓	×	✓
文献[20]方案	✓	✓	✓	✓	×	✓

5.3 性能分析

5.3.1 通信开销

本节主要分析星间组网认证方案的通信开销。受通信距离的影响，星间链路具有极高的通信时延。在认证阶段，相比于数百毫秒的传输时延，认证信令的发送时延及其带宽消耗对方案通信开销的影响可以忽略不计。因此，对于卫星网络这一特殊认证场景，本文主要通过完成认证所需会话次数来对各方案的通信开销进行比较，表 4 列举了不同方案的对比结果。其中，如果认证方案需要注册步骤，阶段 1 表示首次身份认证所需要的会话次数，阶段 2 表示随后的切换认证所需的会话次数；如果

没有注册步骤，阶段 1 表示单次认证所需会话次数，阶段 2 中用“—”表示无此步骤。

由表 4 可知，相比于其他方案，本文方案由于在认证预计算阶段已经预先完成了部分认证参数的传递与计算，在已注册认证信息之后的切换认证过程中，只需要 2 次星间会话即可完成星间身份认证与密钥协商。因此，本文方案在以高通信时延为特点的卫星网络场景中具有更大优势。

表 4　　各方案完成认证所需会话次数

方案	阶段 1/次	阶段 2/次
本文方案	3	2
文献[17]方案	5	3
文献[18]方案	5	—
文献[19]方案	3	—
文献[20]方案	4	—

5.3.2　计算开销

本节主要分析星间组网认证方案的计算开销。由于各方案涉及较多的自定义参数及其对应的计算函数，无法对各方案的计算复杂度进行直接比较，本文采用与文献[21]相同的关键计算比较法对各方案的计算复杂度进行对比，如表 5 所示。其中，BL 代表一次分组加密，H 代表一次散列运算，M 代表一次消息验证码运算，C 代表一次比较运算。

表 5　　各方案完成认证所需计算开销

方案	阶段 1	阶段 2
本文方案	2BL+2H+2M+2C	1M+2C
文献[17]方案	2BL+2H+2M+2C	1H+1M+3C
文献[18]方案	2H+2M+2C	—
文献[19]方案	2BL+2M+2C	—
文献[20]方案	2H+2M+3C	—

如表 5 所示，当新入轨 LEO 在 GEO 处完成认证信息注册后，凭借基于轨位预测技术设计的认证预计算机制，本文方案实现了卫星认证参数的预计算。在后续的认证过程中，卫星只要将收到的认证参数与预计算得到的参数进行简单的序列比较以及进行少量计算就能完成身份认证，不需要进行参数的现场计算与检验，有效地减少了卫星在认证阶段的计算开销。

为进一步对各方案的计算开销进行比较，本文对各方案进行了仿真实验。在仿真实验中，统一采用 i5 4590 + 8 GB RAM 的实验环境，将 SM3-256 bit 作为散列函数、SM3-HMAC-256 bit 作为 MAC 计算函数、SM4-128 bit 作为分组加密算法，将随机数的长度限制为 128 bit、时间戳（序列号）的长度限制为 48 bit。图 4 为各方案完成一定次数的身份认证，计算和验证认证参数所耗费的时间。仿真结果表明，相比于其他方案，本文方案在认证阶段所需的参数计算时间更少。

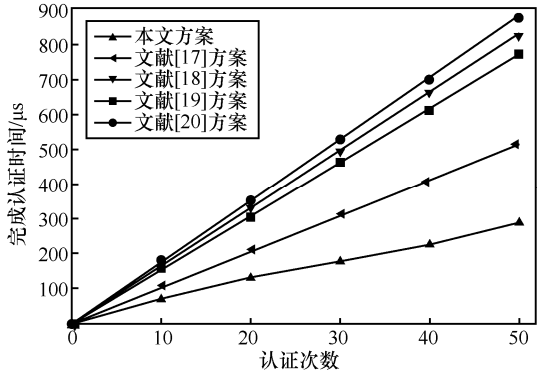

图 4　各方案完成认证的计算时间

6　结束语

本文针对双层卫星网络高、低轨卫星间的安全组网问题，基于对称加密，设计了一种安全、高效的星间组网认证方案。本文方案充分考虑了卫星网络时钟高度同步、卫星轨道可预测的场景特点，设置了认证预计算机制，在保证安全的前提下，通过预计算认证参数有效地缓解了卫星在认证阶段的计算压力。理论分析表明，本文方案除了提供双向认证、抵御重放攻击、抵御拒绝服务攻击外，还能保证会话的前向/后向安全性及卫星身份的匿名性。同时，与同类方案相比，本文方案在提供同等安全性的基础上，具有更低的计算和通信开销，更适用于资源有限的卫星场景中。

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] 廖勇, 樊卓宸, 赵明. 空间信息网络安全协议综述[J]. 计算机科学, 2017, 44(4):202-206.
LIAO Y, FAN Z C, ZHAO M. Survey on security protocol of space information networks[J]. Computer Science, 2017, 44(4):202-206.

[3] 易克初, 李怡, 孙晨华, 等. 卫星通信的近期发展与前景展望[J]. 通信学报, 2015, 36(6):157-172.

YI K C, LI Y, SUN C H, et al. Recent development and its prospect of satellite communications[J]. Journal on Communications, 2015, 36(6):157-172.

[4] LIU J, LIU W, QIANHONG W U, et al. Survey on key security technologies for space information networks[J]. Journal of Communications & Information Networks, 2016, 1(1):72-85.

[5] CHOWDHURY R A, BARAS J S, HADJITHEODOSIOU M. An authentication framework for a hybrid satellite network with resource constrained nodes[C]//International Conference on Space Information Technology. 2006.

[6] 任方, 马建峰, 郝选文. 空间信息网基于证书的混合式公钥基础设施[J]. 吉林大学学报(工学版), 2012, 42(2):440-445.
REN F, MA J F, HAO X W. Certificate-based hybrid public key infrastructure for space information net-works[J]. Journal of Jilin University (Engineering Edition), 2012, 42(2):440-445.

[7] ZHONG Y T, MA J F. A highly secure identity-based authenticated key-exchange protocol for satellite communication[J]. Journal of Communications and Networks, 2010, 12(6):592-599.

[8] ZHANG Y, CHEN J, HUANG B. Security analysis of an authentication and key agreement protocol for satellite communications[J]. International Journal of Communication Systems, 2015, 27(12): 4300- 4306.

[9] QI M, CHEN J. An enhanced authentication with key agreement scheme for satellite communication systems[J]. International Journal of Satellite Communications & Networking, 2018, 36(3):296-304.

[10] VOSSAERT J, LAPON J, DE D B, et al. Symmetric key infrastructure for authenticated key establishment between resource constrained nodes and powerful devices[J]. Security & Communication Networks, 2016, 9(2):106-117.

[11] LEE C C, LI C T, CHANG R X. A simple and efficient authentication scheme for mobile satellite communication systems[J]. International Journal of Satellite Communications & Networking, 2012, 30(1):29-38.

[12] ZHANG Y, CHEN J, HUANG B. An improved authentication scheme for mobile satellite communication systems[J]. International Journal of Satellite Communications & Networking, 2015, 33(2):135-146.

[13] TSAI J L, LO N W, WU T C. Secure anonymous authentication scheme without verification table for mobile satellite communication systems[J]. International Journal of Satellite Communications & Networking, 2015, 32(5):443-452.

[14] YOON E J, YOO K Y, HONG J W, et al. An efficient and secure anonymous authentication scheme for mobile satellite communication systems[J]. EURASIP Journal on Wireless Communications & Networking, 2011, 2011(1):86.

[15] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2):198-208.

[16] 王聪. 安全协议原理与验证[M]. 北京: 北京邮电大学出版社, 2011.
WANG C. Principle and verification of security protocol[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2011.

[17] SAXENA N, CHAUDHARI N S. Secure-AKA: an efficient AKA protocol for UMTS networks[J]. Wireless Personal Communications, 2014, 78(2):1345-1373.

[18] SAXENA N, THOMAS J, CHAUDHARI N S. ES-AKA: an efficient and secure authentication and key agreement protocol for UMTS networks[J]. Wireless Personal Communications, 2015, 84(3):1-32.

[19] HUANG Y L, SHEN C Y, SHIEH S W. S-AKA: a provable and secure authentication key agreement protocol for UMTS networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(9):4509-4519.

[20] OU H H, HWANG M S, JAN J K. A cocktail protocol with the authentication and key agreement on the UMTS[M]. Amsterdam: Elsevier Science Inc. 2010.

[21] 张子剑, 周琪, 张川,等. 新的低轨星座组网认证与群组密钥协商协议[J]. 通信学报, 2018, 39(6):146-154.
ZHANG Z J, ZHOU Q, ZHANG C, et al. New lowearth orbit satellites authentication and group key agreement protocol[J]. Journal on Communications, 2018, 39(6): 146-154.

[作者简介]

朱辉（1981− ），男，河南周口人，博士，西安电子科技大学教授、博士生导师，主要研究方向为数据安全与隐私保护、安全方案及协议设计、网络及应用安全。

武衡（1992− ），男，山西盂县人，西安电子科技大学硕士生，主要研究方向为安全方案及协议设计。

赵海强（1978− ），男，湖北宜昌人，中国电子科技集团公司第五十四研究所硕士生，高级工程师，主要研究方向为网络安全技术。

赵玉清（1994− ），女，河北石家庄人，西安电子科技大学硕士生，主要研究方向为安全方案及协议设计。

李晖（1968− ），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。