基于位置密钥的增强型北斗用户设备接入认证协议

曹进[1]，卜秋雨[1]，杨元元[1]，李晖[1]，刘樵[1]，马懋德[2]
（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；
2. 卡塔尔大学工程学院，多哈 999043）

摘 要：为解决现有北斗用户设备接入协议中认证时延长等缺陷以及满足用户隐私保护的需求，创新性地结合位置信息，提出一种增强型用户设备接入认证协议，实现用户设备和北斗指控中心间的双向认证和会话密钥协商。利用用户设备的位置信息和主密钥形成双因子，所提协议在一定程度上避免了认证过程中用户设备被俘获所导致主密钥泄露的安全问题。Scyther 工具验证表明，所提协议可以满足所提出的安全需求，且具有较小的性能开销，适于节点资源受限的北斗导航卫星系统。

关键词：北斗卫星导航系统；位置密钥；双因子；接入认证
中图分类号：TP302
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022214

Enhanced Beidou user equipment access authentication protocol based on location key

CAO Jin[1], BU Qiuyu[1], YANG Yuanyuan[1], LI Hui[1], LIU Qiao[1], MA Maode[2]
1. School of Cyber Engineering, Xidian University, Xi'an 710071, China
2. College of Engineering, Qatar University, Doha 999043, Qatar

Abstract: In order to solve the shortcomings of the existing Beidou user equipment access solutions such as prolonged authentication, and in response to the need of user privacy protection, a user equipment access authentication protocol based on location key was proposed, which realized the mutual authentication and session key negotiation between entities. Combining Beidou's location information and master key to form a two-factor, the proposed protocol solved the security problem of the master key leaking due to the equipment being captured during the authentication process to some extent. The proposed protocol can meet different security requirements through the verification of the Scyther formal tool. Compared with other similar schemes, it has better performance overhead, and is suitable for Beidou satellite navigation system with limited node resources.

Keywords: Beidou satellite navigation system, location key, two-factor, access authentication

0 引言

随着地面 5G 移动通信技术的快速发展，人们对面向 6G 的未来通信场景提出了更高要求。作为地面通信网络的补充，卫星网络因其覆盖范围广、吞吐量大、部署灵活等特点受到人们的广泛关注[1]。利用卫星网络保障用户设备在偏远山区、荒漠远洋等地的安全接入，为电力勘测、应急救援等领域提供了技术上的支撑，有利于促进天地一体化信息网络的高度融合与深度互联[2-3]。

北斗导航卫星系统由我国自主研制，是继美国的 GPS、俄罗斯的 GLONASS 之后第三个成熟、独

收稿日期：2022−07−07；**修回日期**：2022−10−12
基金项目：国家自然科学基金资助项目（No.62172317, No.U1836203, No.61902297）；陕西省重点产业创新链（群）−工业领域基金资助项目（No.2020ZDLGY08-08）
Foundation Items: The National Natural Science Foundation of China (No.62172317, No.U1836203, No.61902297), The Important Industry Innovation Research Funded by Shaanxi Province (No.2020ZDLGY08-08)

立的卫星导航系统，是我国重要的空间基础设施[4]。其中，北斗三号卫星导航系统由 24 颗中地球轨道（MEO, middle earth orbit）卫星、3 颗地球静止轨道（GEO, geostationary earth orbit）卫星、3 颗倾斜地球同步轨道（IGSO, inclined geosynchronous orbit）卫星构成。MEO 卫星主要负责提供全球范围内的定位导航、国际搜救、短报文通信等服务；GEO 卫星主要提供区域性的精密授时、位置报告等功能；IGSO 卫星可以对 GEO 卫星进行区域互补[5]。

近年来，随着信息网络的快速发展，卫星网络的用户设备接入认证协议逐渐受到研究人员的关注。然而卫星通信具有网络拓扑频繁变化、卫星节点计算和存储能力受限等特点。除此以外，天地一体化信息网络容易受到敌手蓄意攻击和破坏。因此传统地面通信网络等接入认证协议难以适用于卫星网络[6]。综上所述，构建天地一体化信息网络的接入认证架构的重要性不言而喻。

用户设备−卫星−地面控制中心是传统用户设备接入认证的常见架构，根据采用的密码技术的不同，可以将其分为基于公钥密码、对称密码和轻量级算法的接入认证机制。

在基于公钥密码的接入认证机制中，Xue 等[7]提出了一种基于公钥密码算法的卫星用户设备接入认证协议，在该协议中仅需要三次的星地交互即可完成用户设备和地面控制中心的双向认证，降低了信令开销，但是协议中进行了大量的点乘操作，增大了计算开销。Liu 等[8]提出了一种针对不同服务类型、服务场景的用户设备接入认证协议，通过少量的信令交互即可完成双向认证和密钥协商；然而在用户设备的接入认证过程中，大量的签名和验签操作导致计算开销巨大，难以适用于计算资源受限的卫星网络。马军等[9]指出现有的北斗接入认证采用 RSA 算法，导致认证时延较长，因此他们提出了一种基于 SM2 算法的接入认证协议，认证所需的存储空间较小、密钥生成速度快，降低了用户设备在接入认证过程中的认证时延。李昊鹏等[10]和赵东昊等[11]提出了在接入认证过程中加入位置信息来避免假冒攻击的协议，但大量的签名和验签操作会产生较大的计算开销；另外，针对用户设备的身份标识没有进行隐私保护，可能导致用户的身份隐私泄露问题，进而引起针对用户身份的各种攻击，因此该方案并不适合北斗卫星网络。

公钥密码算法往往会带来较大的计算开销，于是研究人员将目光转向对称密码算法。使用对称密码算法来设计用户的接入认证协议，可以减少认证过程中所带来的计算开销，适用于资源受限的卫星网络。朱辉等[12]基于演进的分组交换系统认证与密钥协商（EPS-AKA, evolved packet system based authentication and key agreement）协议提出了一种基于令牌的接入认证机制，实现了用户的随遇接入，但是并没有减少卫星节点的存储开销和地面控制中心的计算开销。Chen 等[13]提出了一种基于离散对数困难问题的认证方案来保证实体之间的通信安全，实现了用户的匿名性和不可追踪性，可以抵抗智能卡被盗的攻击。然而，Kumar 等[14]指出 Chen 等[13]的接入认证协议存在缺陷，用户设备无法向地面控制中心进行身份认证并建立安全的会话密钥。针对此问题，Kumar 等[14]提出了一种移动卫星动态认证协议，协议中主要采用了对称加密算法、哈希函数以及异或操作，认证过程中的信令开销和计算开销较小，在性能和安全需求之间达到了平衡。

Lin[15]提出了一种轻量级的移动卫星通信系统动态认证协议，该协议中地面控制中心不需要使用用户的验证表和更新表即可完成与卫星用户设备的双向认证，降低了通信系统的开销。Liu 等[16]提出了一种临时身份自我更新的策略，通过哈希函数、异或操作等完成了用户和地面控制中心之间的双向认证，计算成本较低。吴克河等[17]提出了一种轻量级哈希算法和证书相结合的认证协议，保证了消息来源的可靠性，然而协议中签名和验签操作带来了较大的计算开销。Zhao 等[18]提出了一种基于北斗通信网络的无人机接入认证协议，该协议使用单向哈希函数完成无人机和地面控制中心之间的双向认证，计算开销小。然而该协议并未考虑到无人机被捕获时可能导致主密钥泄露，因此攻击者可以通过用户设备直接接入北斗网络中，进而引起严重的信息泄露问题。

基于上述技术分析，本文提出一种增强型用户设备的接入认证协议，其特点如下。

1) 支持用户设备接入北斗卫星网络，实现用户设备和北斗指控中心间的双向认证和会话密钥协商。

2) 在认证过程中，对用户的身份标识信息、位置信息进行保护，满足用户身份隐私保护的需求，避免隐私泄露所带来的安全问题。

3) 利用北斗位置报告的独特性和主密钥形成双因子认证，增强认证的准确性，本文协议在一定程度上可以抵抗用户设备被捕获而造成的主密钥泄露攻击。

4) 采用安全分析和性能分析充分评估本文协议的安全性，使用形式化验证工具 Scyther 证明其安全性。在性能分析方面，从计算开销、带宽开销以及存储开销 3 个方面将本文协议与其他类似协议进行对比，协议分析结果表明，本文协议在性能开销和安全需求之间达到了一种平衡，更加适用于节点资源受限的北斗卫星导航系统。

1 系统模型与安全需求

1.1 系统模型

系统模型如图 1 所示，本文主要研究用户设备在卫星网络下的初始注册和接入认证过程。系统架构主要包括以下实体：北斗卫星导航系统（BDS, Beidou satellite navigation system）、北斗指控中心（BDC, Beidou control）以及用户设备（UE, user equipment）。

北斗导航卫星系统是由不同轨道、不同类型的卫星组成的多层次天基信息网络，计算、存储能力有限，主要负责用户设备和北斗指控中心之间的信息交互。

北斗指控中心由主控站、监测站等构成，是北斗卫星导航系统的主要管理者，负责北斗卫星导航系统的运行控制、实时检测、数据处理等任务[5]。北斗指控中心一般具有较高的计算能力和存储能力，可以承担大量、复杂的运算。

用户设备指各种类型的用户设备，如手持用户设备，可以通过北斗卫星导航系统接入北斗卫星网络，并获得相应的网络服务。

1.2 安全需求

根据所述架构，用户设备通过北斗卫星与地面通信的场景属于无线通信领域，该领域中有 2 种常见的攻击模型：DY（Dolev-Yao）模型和 CK（Canetti-Krawczyk）模型。DY 模型是指攻击者可以对信息网络中的消息进行截获、重放、篡改，并且可以假冒网络中的任意合法实体进行通信。CK 模型指对实体内部的攻击，出现主密钥泄露、会话密钥泄露造成非法用户获得相应的网络服务。用户设备的接入认证具有以下安全需求。

1) 双向认证。网络中的实体需要进行相互认证，BDC 需要确认 UE 的身份，防止非法的用户实体接入网络并获得相应的服务；同时，UE 需要确定 BDC 的身份，防止中间人、假冒攻击等造成用户的相关隐私信息泄露。

2) 密钥协商。在接入认证之后，UE 需要和 BDC 协商出一个会话密钥，便于保障后续通信消息的完整性和机密性。

3) 条件隐私性。用户的条件隐私性主要是针对 UE 的真实身份标识和位置信息进行保护。BDC 生成 UE 临时身份标识，对 UE 的真实身份标识进行匿名保护，且各个临时身份标识之间不具有相关性，保证后续认证消息中 UE 身份的独立性。除此以外，采用临时身份保护序列传递下一次接入认证的临时身份标识，避免恶意实体的追踪行为，增强认证过程的安全性；对 UE 的位置信息进行加密处理，保证位置信息的机密性。

4) 可追责。由于用户隐私保护的需求，本文协议中其他实体和攻击者无法得知 UE 的真实身份标识。然而当 UE 存在恶意行为时，应该具有追责的能力来保障天地一体化信息网络的安全。

5) 前后向安全性。为了保证 UE 在后续通信过

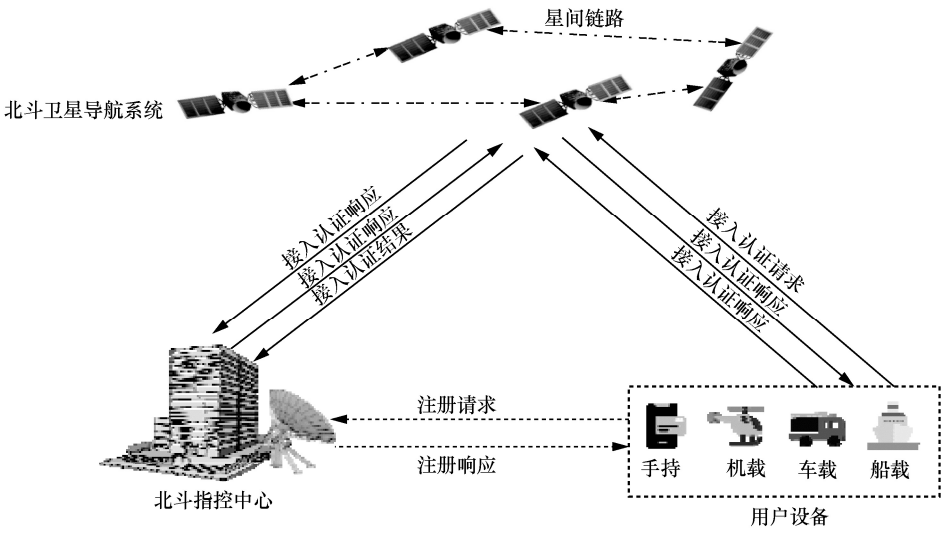

图 1 系统模型

程中会话的机密性和完整性，应当实现密钥的前后向安全性。这意味着即使当前的密钥泄露，攻击者也不能推出之前的会话和将来的会话中使用的密钥，从而无法破解出更多的通信内容。

除此以外，协议还应该能抵抗常见的攻击，如中间人攻击、重放攻击、假冒攻击等。

2　协议设计

2.1　设计思路

针对上述的安全需求，本节提出了一种基于位置密钥的增强型用户设备接入认证协议，主要分为以下 2 个过程：用户设备注册过程和用户设备接入认证过程。

在注册阶段，UE 首先向 BDC 发起注册请求，BDC 收到 UE 的请求之后，通过安全信道下发主密钥 key 和临时身份标识 PID_u，临时身份标识会在初始接入认证时进行更新，便于下一次接入认证时使用。在初始接入认证阶段，UE 和 BDC 利用主密钥 key 派生加密密钥 CK 和位置密钥 AK，CK 用于用户设备的位置信息的机密性保护， AK 用于完成实体之间的双向认证。除此以外，认证过程中主要采用了单向哈希函数和对称加密算法 SM4，通过引入随机数、时间戳、消息认证码、认证响应值，实现了用户设备的接入认证和会话密钥的协商。表 1 列举了用户设备在认证过程中使用的符号及其含义。

表 1　用户设备在认证过程中使用的符号及其含义

符号	含义
K	北斗指控中心的基础密钥
key	用户设备的主密钥
ID_u	用户设备的真实身份标识
PID_u	用户设备的临时身份标识
T	时间戳
L_u	用户设备的位置信息
N_u	用户设备的随机数
N_s	北斗指控中心的随机数
CK	加密密钥
AK	位置密钥
MAC	用户设备侧的消息验证码
HMAC	北斗指控中心侧的消息验证码
RES	用户设备侧的认证响应值
XRES	北斗指控中心侧的认证响应值
AV	认证向量
S_k	会话密钥

2.2　用户设备注册过程

为实现用户设备注册过程，用户设备进行离线注册，北斗指控中心分发主密钥、生成用户接入认证的临时身份标识等相关安全参数，具体过程如图 2 所示。

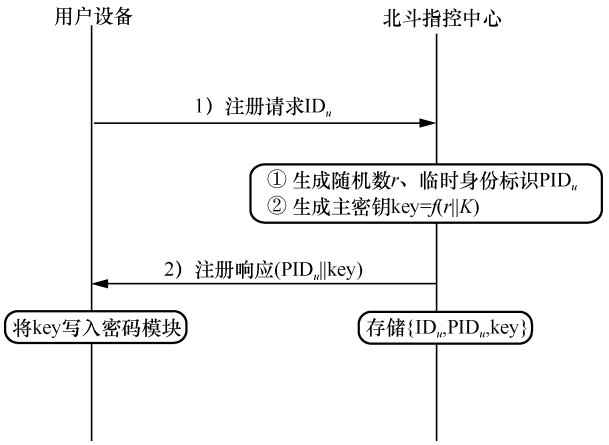

图 2　用户设备注册过程

1) UE 根据用户自身的 ID_u 标识发起注册请求至 BDC。

2) BDC 生成随机数 r、用户设备的临时身份标识 PID_u，结合基础密钥 K，导出用户设备的主密钥 $\mathrm{key}=f(r\|K)$，BDC 保存用户设备的真实身份标识 ID_u、临时身份标识 PID_u 和主密钥 key，并将用户设备的临时身份标识 PID_u 和主密钥 key 分发至用户设备。

3) UE 将收到的用户设备的主密钥 key 写入密码模块。

2.3　用户设备接入认证过程

针对天地一体化信息网络的星地交互时延高、卫星节点资源受限等特点，本节设计了一种基于哈希的轻量级认证协议，如图 3 所示。该协议仅需要少量哈希算法和对称密钥算法就可以完成实体之间的双向认证以及会话密钥协商，降低了系统的计算开销。

1) UE 获取当前的时间 T_1、位置信息 L_u，生成随机数 N_u，结合自身的 ID_u 标识、主密钥 key，计算加密密钥 $\mathrm{CK}=\mathrm{KDF}(\mathrm{key},\mathrm{ID}_u\|T_1)$、位置密钥 $\mathrm{AK}=\mathrm{KDF}(\mathrm{key},\mathrm{PID}_u\|N_u\|L_u)$、消息验证码 $\mathrm{MAC}_1=h(\mathrm{AK},\mathrm{PID}_u\|T_1\|N_u\|L_u)$、认证向量 $\mathbf{AV}_1=\mathrm{PID}_u\|\mathrm{SM}_4(\mathrm{CK},N_u\|L_u)\|\mathrm{MAC}_1\|T_1$，将认证向量 $\mathbf{AV}_1$ 发送至 BDS。

2) BDS 收到认证向量 $\mathbf{AV}_1$，连同自身 $\mathrm{ID}_{\mathrm{BDS}}$ 标识发送至 BDC。

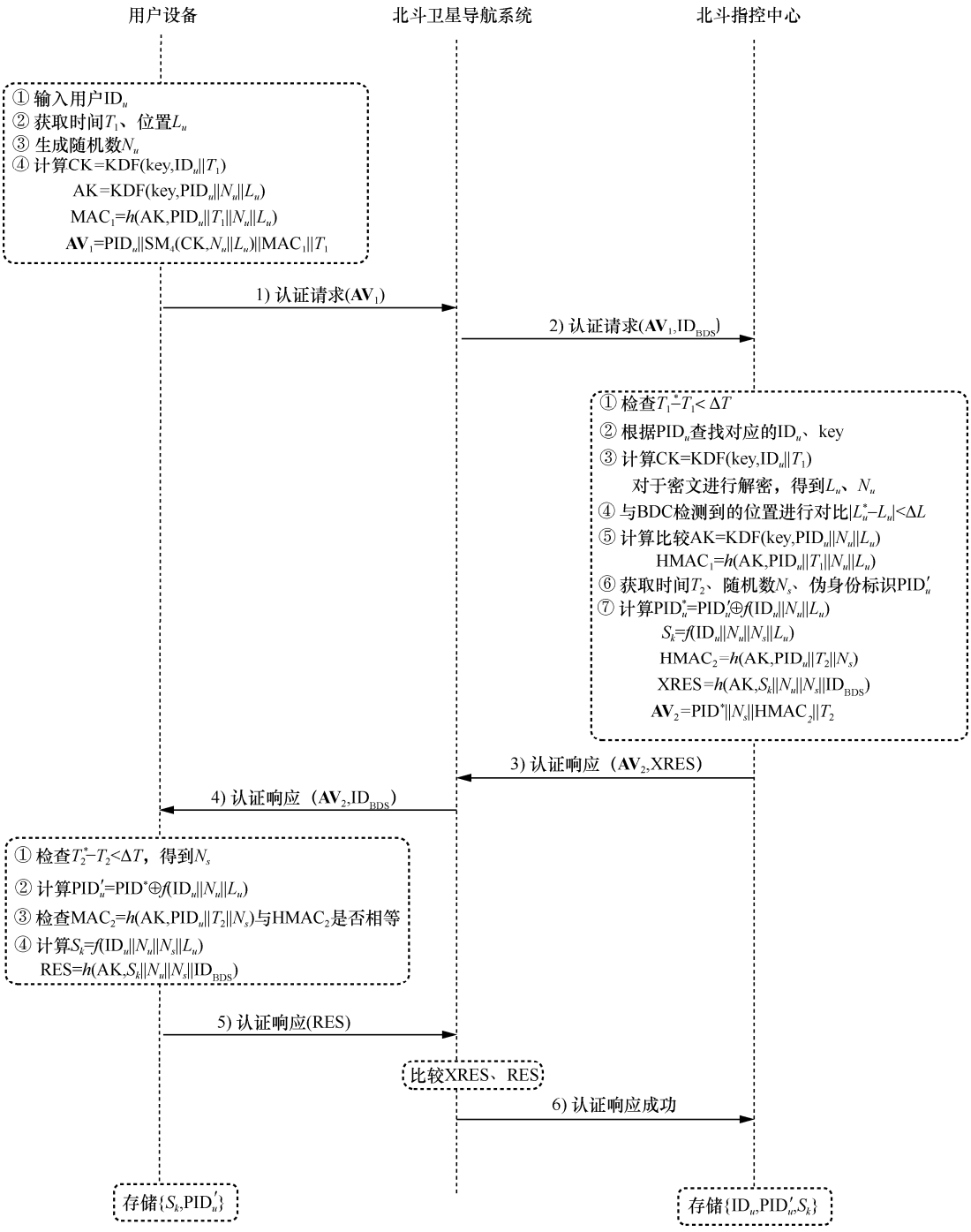

图 3 用户设备接入认证过程

3) BDC 检查时间戳 T_1 的有效性，若有效，则根据 PID_u 查找对应的真实用户标识符 ID_u、key，计算位置解密密钥 $\mathrm{CK}=\mathrm{KDF}(\mathrm{key},\mathrm{ID}_u\|T_1)$，对于认证向量 $\mathbf{AV}_1$ 中的 $\mathrm{SM}_4(\mathrm{CK},N_u\|L_u)$ 进行解密，获得 L_u、N_u，与 BDC 检测到的位置进行对比，看其是否满足 $|L_u^*-L_u|<\Delta L$，ΔL 为预先设定的位置容忍精度，若满足，则计算位置密钥 $\mathrm{AK}=\mathrm{KDF}(\mathrm{key},\mathrm{PID}_u\|N_u\|L_u)$，比较消息认证码 $\mathrm{HMAC}_1=h(\mathrm{AK},\mathrm{PID}_u\|T_1\|N_u\|L_u)$ 是否与收到的 MAC_1 相等，若相等，则获取当前的时间 T_2、生成随机数 N_s 和下次临时身份标识 PID_u'，计算临时身份保护序列 $\mathrm{PID}^*=\mathrm{PID}_u'\oplus f(\mathrm{ID}_u\|N_u\|L_u)$、会话密钥 $S_k=f(\mathrm{ID}_u\|N_u\|N_s\|L_u)$、消息验证码 $\mathrm{HMAC}_2=h(\mathrm{AK},\mathrm{PID}_u\|T_2\|N_s)$、认证响应值

$\mathrm{XRES}=h(\mathrm{AK},S_k\|N_u\|N_s\|\mathrm{ID}_{\mathrm{BDS}})$、认证向量$\mathbf{AV}_2=\mathrm{PID}^*\|N_s\|\mathrm{HMAC}_2\|T_2$，将认证向量$\mathbf{AV}_2$、认证响应值XRES发送至BDS。

4) BDS收到认证向量$\mathbf{AV}_2$和认证响应值XRES，将认证向量$\mathbf{AV}_2$连同自身$\mathrm{ID}_{\mathrm{BDS}}$标识发送至UE。

5) UE检查时间戳T_2的有效性，若有效，则获得N_s、$\mathrm{PID}_u^{'}=\mathrm{PID}^*\oplus f(\mathrm{ID}_u\|N_u\|L_u)$，比较消息认证码$\mathrm{MAC}_2=h(\mathrm{AK},\mathrm{PID}_u\|T_2\|N_s)$是否与收到的$\mathrm{HMAC}_2$相等，若相等，则计算会话密钥$S_k=f(\mathrm{ID}_u\|N_u\|N_s\|L_u)$、认证响应值$\mathrm{RES}=h(\mathrm{AK},S_k\|N_u\|N_s\|\mathrm{ID}_{\mathrm{BDS}})$，将认证响应值RES发送至BDS，UE存储$\{S_k,\mathrm{PID}_u'\}$。

6）BDS收到认证响应值RES，将其与XRES进行比较，若相等，则将认证成功的结果发送至BDC。

7）BDC收到认证成功的结果，BDC存储$\{\mathrm{ID}_u,\mathrm{PID}_u',S_k\}$，随后即可使用会话密钥$S_k$进行保密通信。

3　安全性分析

3.1　非形式化安全分析

本节采用非形式化的方法分析本文协议的安全性，并讨论抵御各种攻击类型的能力。

1) 双向认证。在上述用户设备接入认证过程中，用户设备和北斗指控中心可以进行双向的身份认证。用户设备通过将本地计算的MAC_2和收到的消息验证码HMAC_2进行比较来鉴别北斗指控中心的身份；北斗指控中心通过本地计算的消息验证码HMAC_1和收到的消息验证码MAC_1是否相等来鉴别用户设备的身份，实现了两方实体的身份认证。

2) 条件隐私性。条件隐私性分为用户设备身份的匿名性和用户设备位置信息的机密性。UE的匿名性通过注册过程中生成的临时身份标识PID_u实现，并且在接入认证过程中由北斗指控中心重新生成新的临时身份标识PID_u'，来保障下一次的用户设备接入认证过程中UE身份的匿名性。BDS中不会存储用户的真实身份标识和临时身份标识的映射表，且单向哈希算法不能通过反向求解获得用户的真实身份。因此对于BDS以及其他用户和敌手，可以实现用户身份匿名性。位置信息的机密性通过在接入认证过程中生成加密密钥CK对位置信息进行加密，对于其他用户和敌手来说，因为其不持有正确ID_u，无法计算出正确的加密密钥，所以无法解密获得用户设备的位置。

3) 可追责与不可链接性。BDC本地存储着与临时身份标识PID_u相对应的真实身份标识ID_u，所以BDC可以获得用户的真实身份，实现用户设备恶意行为的可追踪性。因为链路的开放性，公共信道中的消息容易被攻击者所捕获，而攻击者有可能从多次相同的认证信息中链接到某个实体。而在本文协议中，传递的认证消息在每一步骤后均进行了更新，对于攻击者来说是完全随机的，因此不可能从消息中完成对于实体身份的关联。

4) 抵抗重放攻击。在用户设备接入认证过程中，UE发送的认证向量$\mathbf{AV}_1=\mathrm{PID}_u\|\mathrm{SM}_4(\mathrm{CK},N_u\|L_u)\|\mathrm{MAC}_1\|T_1$和BDC发送的认证向量$\mathbf{AV}_2=\mathrm{PID}^*\|N_s\|\mathrm{HMAC}_2\|T_2$中加入了时间戳，保证了消息的新鲜性。认证双方实体可以通过是否含有相同时间戳消息来快速鉴别出攻击者的攻击行为，因此，本文协议可以抵抗重放攻击。

5) 抵抗中间人攻击。在本文协议中，只有用户和北斗指控中心知晓用户的真实身份和对应的主密钥，用户在认证请求消息中使用匿名身份标识PID_u，攻击者无法获得用户设备的真实身份标识ID_u和主密钥key。攻击者无法根据截获的消息解密用户和北斗指控中心的会话内容，也就无法假冒其中一方与另一方进行通信。因此，本文协议可以抵抗中间人攻击。

6) 前后向安全。在本文协议中，生成会话密钥时都使用新的随机数，各会话密钥之间独立。攻击者并不能推出之前的会话和将来的会话中的密钥，无法破解出更多的通信内容。因此，本文协议可以实现前后向安全。

7) 双因子认证。本文协议结合北斗位置报告服务，利用用户设备的位置信息和主密钥形成双因子，在一定程度上避免了在认证过程中用户设备被俘获可能导致的主密钥泄露的安全问题，实现了用户设备和北斗指控中心之间的双向认证和会话密钥的协商。

3.2　形式化安全分析

本节采用形式化工具Scyther验证本文协议的安全性，该工具用于识别协议中常见的漏洞，形成攻击输出图[19]。Scyther内部设置单向哈希函数、对称加解密等操作，方便将协议转换为spdl（安全协议描述）语言。本文涉及用户注册和接入认证2个阶

段，由于用户离线完成注册流程，因此该流程不进行形式化验证。

首先，声明协议名和角色集；其次，声明角色中的变量、收发认证消息和具有的安全属性；最后，运行协议进行形式化验证[20]。Scyther 中各个角色从自身角度检测是否得到满足，若满足该安全需求，验证输出结果中的 Status（状态）为 Verfied（通过）；否则为 Falsified（失败）。

针对用户设备的接入认证流程，本文使用 Scyther 工具进行形式化验证。协议中涉及三方实体，即 UE、BDC 和 BDS。对通信实体的安全属性，如 Secret（机密性）、Alive（存活性）、Weakagree（弱一致性）、Niagree（非单射一致攻击）和 Nisynch（前向安全）等进行声明，验证结果如图 4 所示。

图 4 用户设备接入认证流程 Scyther 验证结果

由图 4 可知，在 Scyther 声明的 Secret、Alive、Weakagree、Niagree 和 Nisynch 属性范围内均没有发现任何攻击。结果表明，本文协议实现了双向认证和用户身份的隐私保护，具有前后向安全性，并且可以抵抗常见的协议攻击，如中间人攻击、重放攻击等，保证了通信的机密性和完整性。

4 性能分析

在性能分析阶段，本文首先从多个安全属性的角度对本文协议和其他相似协议进行分析对比；然后从计算开销、带宽开销、存储开销 3 个方面对本文协议和其他相似协议进行分析。

4.1 安全性对比

本节针对本文协议和其他相似协议进行了安全性对比，分析结果如表 2 所示。从表 2 可以看出，文献[11]、文献[17]协议并没有对用户的真实身份标识进行保护，容易造成用户隐私信息的泄露。文献[12]、文献[14]针对天地一体化信息网络场景下提出的接入认证协议不具有后向安全性，可以推断出未来的会话密钥，带来了严重的安全问题。文献[8]、文献[12]协议不能抵抗主密钥泄露攻击，甚至可以计算出当前的会话密钥，通信信息的机密性和完整性将受到威胁。本文协议利用北斗位置报告的独特性，将用户设备的位置信息和主密钥相结合形成双因子，并将位置信息加入认证密钥当中，在一定程度上可以抵抗由于用户设备被捕获而造成主密钥泄露攻击的情况，有效地保障了通信过程中协议的安全性和可靠性。

表 2 安全性对比分析结果

协议	双向认证	条件隐私	不可链接性	前后向安全性	双因子认证
文献[8]	√	√	√	√	×
文献[11]	√	×	√	×	×
文献[12]	√	√	√	×	×
文献[14]	√	√	√	×	√
文献[17]	√	×	√	×	×
本文协议	√	√	√	√	√

4.2 计算开销

本文在计算开销方面忽略级联、异或操作时间，只考虑以下计算时间：哈希运算 T_{H}、对称加解密运算 T_{s}、非对称加密运算 T_{enc}、非对称解密运算 T_{dec}、签名运算 T_{sig}、验签运算 T_{ver}、密钥生成函数运算 T_{KDF}、点乘运算 T_{mul}，通过构建一个仿真平台来测试以上密码学算法的开销。

选择两台性能不同的计算机，一台处理器为 Intel（R） Core（TM）m3-6Y30 CPU @0.9 GHz，模拟计算资源、存储资源受限的用户设备/卫星；另一台处理器为 Core（TM） i7-7500U CPU @2.70 GHz，模拟地面控制中心。所有密码算法基于 openssl-1.0.2e[21] 实现，将每个密码学算法运行 1 000 次，然后取平均运行时间作为该密码学算法的计算开销，如表 3 所示[22]。各协议的计算开销如表 4 所示。

表 3　　每个密码学算法的平均运行时间

运算类型	用户设备或卫星/μs	地面控制中心/μs	运算类型	用户设备或卫星/μs	地面控制中心/μs
T_{H}	2.39	1.21	T_{sig}	1.20×10^{3}	0.73×10^{3}
T_{s}	2.26	1.05	T_{ver}	0.81×10^{3}	0.44×10^{3}
T_{enc}	8.97	5.32	T_{KDF}	2.42	1.23
T_{dec}	0.08	0.03	T_{mul}	1.00×10^{3}	0.52×10^{3}

表 4　　基于密码学算法的计算开销

协议	用户设备	卫星	地面控制中心	总计算开销/μs
文献[8]	$3T_{\mathrm{mul}}+4T_{\mathrm{H}}+T_{\mathrm{sig}}+2T_{\mathrm{ver}}+T_{\mathrm{s}}$	—	$3T_{\mathrm{mul}}+4T_{\mathrm{H}}+T_{\mathrm{sig}}+2T_{\mathrm{ver}}+T_{\mathrm{s}}$	9 007.71
文献[11]	$T_{\mathrm{H}}+T_{\mathrm{enc}}+T_{\mathrm{sig}}+T_{\mathrm{dec}}+T_{\mathrm{ver}}$	—	$T_{\mathrm{H}}+T_{\mathrm{enc}}+T_{\mathrm{sig}}+T_{\mathrm{dec}}+T_{\mathrm{ver}}$	3 198
文献[12]	$4T_{\mathrm{H}}$	T_{s}	$6T_{\mathrm{H}}+T_{\mathrm{s}}$	20.13
文献[14]	$3T_{\mathrm{mul}}+9T_{\mathrm{H}}+T_{\mathrm{s}}$	—	$3T_{\mathrm{mul}}+6T_{\mathrm{H}}+T_{\mathrm{s}}$	4 592.08
文献[17]	$T_{\mathrm{s}}+2T_{\mathrm{H}}+T_{\mathrm{sig}}+T_{\mathrm{ver}}$	—	$T_{\mathrm{s}}+2T_{\mathrm{H}}+T_{\mathrm{sig}}+T_{\mathrm{ver}}$	3 190.51
本文协议	$2T_{\mathrm{KDF}}+5T_{\mathrm{H}}+T_{\mathrm{s}}$	—	$2T_{\mathrm{KDF}}+5T_{\mathrm{H}}+T_{\mathrm{s}}$	28.61

图 5 绘制了各协议在接入认证阶段计算开销随认证次数增加时的变化。本文协议与文献[8]、文献[11]、文献[14]、文献[17]协议相比具有较大优势。本文协议基于哈希函数、KDF 算法、对称加密机制，避免了公钥密码体制的签名验签、点乘操作，虽然计算开销略高于文献[12]协议，但是在存储开销、带宽开销方面相比文献[12]协议具有显著优势。

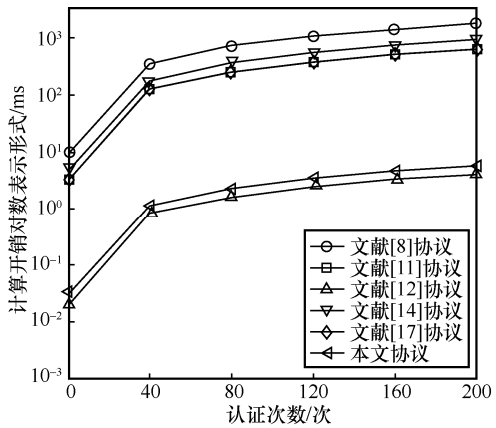

图 5　各协议在接入认证阶段计算开销随认证次数增加时的变化

4.3　带宽开销

为了公平起见，本节将各协议的带宽开销在 AES-128 bit 同等安全级别进行比较。对称加密算法的密钥长度为 SM4-128 bit；公钥密码算法的公钥长度为 3 072 bit，私钥长度为 256 bit；椭圆曲线的密钥长度为 320 bit; 哈希函数的输出长度为 128 bit; KDF 的输出长度为 SM3-256 bit；用户设备身份标识、临时身份标识的长度为 128 bit；卫星身份标识的长度为 32 bit；随机数的长度为 128 bit；位置信息的长度为 128 bit；时间戳的长度为 32 bit。各协议的带宽开销对比如表 5 所示。

表 5　　各协议的带宽开销对比

协议	用户设备/bit	卫星/bit	地面控制中心/bit	总带宽开销/bit
文献[8]	7 072	—	7 232	14 304
文献[11]	3 840	—	3 712	7 552
文献[12]	672	32	640	1 344
文献[14]	608	64	448	1 120
文献[17]	768	—	768	1 536
本文协议	416	64	544	1 024

为了更加直观地展现各协议的带宽开销，本节将其绘制成对数形式的折线，结果如图 6 所示。从图 6 可以看出，文献[8]、文献[11]协议中的带宽开销较大，因为这 2 种协议主要采用了公钥密码算法，通信过程需要发送相关签名数据、点乘运算结果等，增加了协议所需的带宽开销。与其他协议相比，本文协议的带宽开销最低，更加适用于资源受限的用户设备/卫星的天地一体化信息网络。

4.4　存储开销

本节将计算在接入认证过程中所要花费的存储开销，协议中需要存储的相关身份标识、会话密钥等关键信息便于后续完成双向认证。为了公平起见，在 AES-128 bit 同等安全级别进行比较，具体的各种

密码学操作所需要的开销与 4.3 节中的定义保持一致。各协议在接入认证阶段的存储开销对比如表 6 所示。

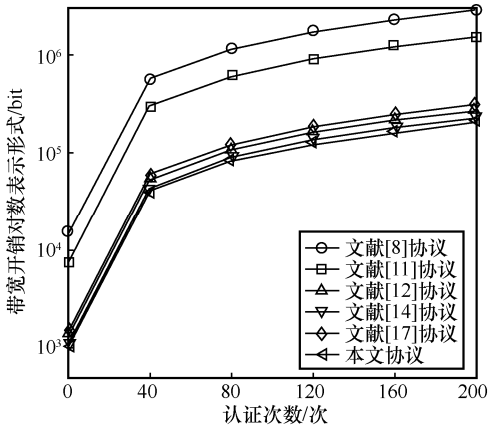

图 6 各协议的带宽开销对比

表 6 各协议在接入认证阶段的存储开销对比

协议	用户设备/bit	卫星/bit	地面控制中心/bit	总存储开销/bit
文献[8]	3 482	—	6 656	10 138
文献[11]	3 840	—	3 840	7 680
文献[12]	3 84	160	544	1 088
文献[14]	3 328	32	640	4 000
文献[17]	3 456	—	3 456	6 912
本文协议	256	32	384	704

各协议的存储开销对比如图 7 所示。从图 7 可以看到，文献[8]、文献[11]、文献[17]协议因为采用公钥密码算法，需要存储实体的私钥和公钥，产生了较大的存储开销。本文协议采用轻量级算法，在用户设备侧存储临时身份标识和会话密钥；在北斗指控中心侧存储用户设备的真实身份标识、临时身份标识、会话密钥，存储开销远低于其他协议，更加适用于资源受限的卫星节点/用户设备的天地一体化信息网络。

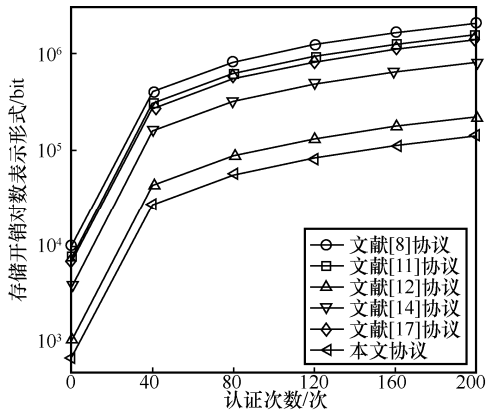

图 7 各方案的存储开销对比

5 结束语

本文针对现有的用户设备接入认证协议的不足和安全需求，提出了一种基于位置密钥的增强型用户设备接入认证协议，使用户设备安全高效地接入网络获取服务。在认证过程中，利用北斗位置报告的独特性和主密钥形成双因子认证，增强了认证的准确性，一定程度上可以抵抗用户设备被捕获而造成的主密钥泄露攻击。通过 Scyther 进行形式化验证可以看出，本文协议可以抵抗各种协议攻击并且满足用户的条件隐私性、抗重放攻击等安全需求。此外，本文协议仅使用哈希算法和对称加密算法来实现用户设备和北斗指控中心之间的双向认证，可以有效地降低协议的认证开销，因此更加适用于节点资源受限的北斗卫星导航系统。

参考文献：

[1] ALSHARIF M, KELECHI A, ALBREEM M, et al. Sixth generation (6G) wireless networks: vision, research activities, challenges and potential solutions[J]. Symmetry, 2020, 12: 676.

[2] 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.

[3] SHENG M, ZHOU D, LIU R Z, et al. Resource mobility in space information networks: opportunities, challenges, and approaches[J]. IEEE Network, 2019, 33(1): 128-135.

[4] 袁冰清, 蔡芸云, 王英翔. 浅析北斗导航卫星系统[J]. 中国无线电, 2022(2): 46-47.
YUAN B Q, CAI Y Y, WANG Y X. Elementary analysis of Beidou navigation satellite system(BDS)[J]. China Radio, 2022(2): 46-47.

[5] 王斯梁, 冯暄, 陈翼, 等. 北斗导航系统信息安全研究[J]. 信息安全研究, 2020, 6(12): 1068-1073.
WANG S L, FENG X, CHEN Y, et al. Research of information security in Beidou navigation system[J]. Journal of Information Security Research, 2020, 6(12): 1068-1073.

[6] 曾勇, 王驭, 徐文斌, 等. 天地一体化信息网络无线链路安全防护技术探讨[J]. 信息安全与通信保密, 2020, 18(10): 100-106.
ZENG Y, WANG Y, XU W B, et al. Discussion on the wireless link security protection technology of the space-ground integrated information network[J]. Information Security and Communications Privacy, 2020, 18(10): 100-106.

[7] XUE K P, MENG W, LI S H, et al. A secure and efficient access and handover authentication protocol for Internet of things in space information networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 5485-5499.

[8] LIU Y, NI L Q, PENG M G. A secure and efficient authentication protocol for satellite-terrestrial networks[J]. IEEE Internet of Things Journal, 2022, doi: 10.1109/JIOT.2022.3152900.

[9] 马军, 黄慧, 夏传福, 等. 基于标识认证和 SM2 算法的用户终端接

入认证协商协议[J]. 电子设计工程, 2020, 28(19): 67-70, 75.
MA J, HUANG H, XIA C F, et al. Beidou terminal access authentication negotiation protocol based on identity authentication and SM2 algorithm[J]. Electronic Design Engineering, 2020, 28(19): 67-70, 75.
[10] 李昊鹏, 陈立云, 卢昱. 基于北斗的军事物联网身份认证方案研究[J]. 计算机应用研究, 2018, 35(8): 2431-2434.
LI H P, CHEN L Y, LU Y. Research on identity authentication scheme based on Beidou in military Internet of Things[J]. Application Research of Computers, 2018, 35(8): 2431-2434.
[11] 赵东昊, 卢昱, 王增光. 北斗战场通信网络身份认证方法[J]. 现代防御技术, 2019, 47(3): 99-105.
ZHAO D H, LU Y, WANG Z G. Identity authentication method of “Beidou” battlefield communication network[J]. Modern Defence Technology, 2019, 47(3): 99-105.
[12] 朱辉, 陈思宇, 李凤华, 等. 面向低轨卫星网络的用户随遇接入认证协议[J]. 清华大学学报(自然科学版), 2019, 59(1): 1-8.
ZHU H, CHEN S Y, LI F H, et al. User random access authentication protocol for low earth orbit satellite networks[J]. Journal of Tsinghua University (Science and Technology), 2019, 59(1): 1-8.
[13] CHEN Y L, CHEN J H. An enhanced dynamic authentication scheme for mobile satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2021, 39(3): 250-262.
[14] KUMAR U, GARG M. A note on an enhanced dynamic authentication scheme for mobile satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2022, 40(5): 317-329.
[15] LIN H Y. Efficient dynamic authentication for mobile satellite communication systems without verification table[J]. International Journal of Satellite Communications and Networking, 2016, 34(1): 3-10.
[16] LIU Y C, ZHANG A X, LI S H, et al. A lightweight authentication scheme based on self-updating strategy for space information network[J]. International Journal of Satellite Communications and Networking, 2017, 35(3): 231-248.
[17] 吴克河, 李岩, 崔文超, 等. 基于商密算法的北斗短报文安全通信协议研究[J]. 计算机与数字工程, 2018, 46(11): 2291-2295, 2374.
WU K H, LI Y, CUI W C, et al. Research of Beidou short message security communication protocol based on commercial password[J]. Computer & Digital Engineering, 2018, 46(11): 2291-2295, 2374.
[18] ZHAO D H, LU Y, LIU X G, et al. Design of emergency UAV network identity authentication protocol based on Beidou[J]. MATEC Web of Conferences, 2021, 336: 04004.
[19] 韩旭, 陆思奇, 程庆丰. 形式化工具 Scyther 优化与实例分析[J]. 信息安全研究, 2016, 2(3): 272-279.
HAN X, LU S Q, CHENG Q F. The improvement and instance analysis of the formal verification tool scyther[J]. Journal of Information Security Research, 2016, 2(3): 272-279.
[20] 石小平, 马如慧, 曹进, 等. 面向卫星网络断续连通场景的接入和切换认证机制[J]. 天地一体化信息网络, 2021, 2(3): 24-34.
SHI X P, MA R H, CAO J, et al. Access and handover authentication in intermittent connection scenario of satellite network[J]. Space-Integrated-Ground Information Networks, 2021, 2(3): 24-34.
[21] BERINGER L, PETCHER A, KATHERINE Q Y, et al. Verified correctness and security of OpenSSL HMAC[C]//Proceedings of 24th USENIX Security Symposium. Berkeley: USENIX Association, 2015: 207-221.
[22] MA R H, CAO J, FENG D G, et al. LAA: lattice-based access authentication scheme for IoT in space information networks[J]. IEEE Internet of Things Journal, 2020, 7(4): 2791-2805.

[作者简介]

曹进（1985− ），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为 4G/5G 网络、天地一体化信息网络安全性及认证协议设计与分析等。

卜秋雨（1998− ），女，甘肃兰州人，西安电子科技大学硕士生，主要研究方向为 4G/5G 网络、天地一体化网络用户设备身份认证等。

杨元元（1998− ），女，河南安阳人，西安电子科技大学硕士生，主要研究方向为 4G/5G 网络、天地一体化信息网络安全认证机制等。

李晖（1968− ），男，陕西西安人，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、信息理论和网络编码等。

刘樵（1989− ），男，陕西咸阳人，博士，西安电子科技大学副教授，主要研究方向为物理层安全、5G 安全、协同通信网络安全等。

马懋德（1957− ），男，博士，卡塔尔大学教授、博士生导师，主要研究方向为无线网络和网络安全。