

面向卫星网络断续连通场景的接入和切换认证机制

石小平¹, 马如慧¹, 曹 进¹, 李 晖¹, 陈李兰¹, 李凤华^{2,3}

(1.西安电子科技大学网络与信息安全学院, 陕西 西安 710126;

2.中国科学院信息工程研究所, 北京 100093;

3.中国科学院大学网络空间安全学院, 北京 100049)

摘 要: 针对低轨卫星网络链路断续连通的问题提出一种接入认证、通信恢复和卫星切换方案。该方案基于对称密码体制设计, 采用单向散列算法、异或操作和时间戳保护机制, 在实现安全接入认证的前提下, 降低信令开销、带宽开销和计算开销。针对链路中断情况, 该方案基于卫星网络和用户的当前会话密钥, 快速安全地恢复通信, 保障服务质量。通过轨道预测技术, 根据当前会话密钥和随机数实现卫星接入点间安全切换, 减少卫星切换过程中的通信成本。该方案还可实现用户身份匿名性, 成功认证后刷新临时身份用于下一次认证。

关键词: 天地一体化信息网络; 接入认证; 切换; 断续连通

中图分类号: TN302

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2021028

Access and Handover Authentication in Intermittent Connection Scenario of Satellite Network

SHI Xiaoping¹, MA Ruhui¹, CAO Jin¹, LI Hui¹, CHEN Lilan¹, LI Fenghua^{2,3}

1.School of Cyber Engineering, Xidian University, Xi'an 710126, China

2.Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

3.School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: This article disclosed an authentication method for access and handover in a low-orbit satellite network intermittent connection scenario. The scheme was based on a symmetrical cryptographic system. Based on hash function, XOR operation and timestamp, the safe access of the terminal to the satellite network was ensured. It reduced signaling overhead, bandwidth overhead, and computing overhead as well. In view of the link interruption, the solution was based on the current session key between the user and satellites to quickly and safely resume communication to ensured the quality of service. Through the orbit prediction technology, according to the current session key between the user and satellites and random number, the safe switching between satellites was realized, and the communication cost during the satellite switching process was reduced. The scheme realized the anonymity of user identity, and refreshed the temporary identity for the next authentication after successful authentication.

Keywords: space-integrated-ground information network, access authentication, handover, intermittent connection scenario

1 引言

天地一体化信息网络是以地基信息网络为基础、以天基信息网络为主体、实现深空信息网络可互联的一体

化综合信息网络, 由不同轨道、不同类型、不同性能的星座组成互联的骨干网/接入网并覆盖全球。它通过星间链路和星地链路实现各种用户终端、海陆空及近地地

收稿日期: 2021-07-31; **修回日期:** 2021-08-28

基金项目: 国家自然科学基金面上项目 (No. 61772404); 陕西省重点产业创新链 (群)-工业领域项目 (No. 2020ZDLGY08-08); 国家自然科学基金重点类项目 (No. U1836203)

Foundation Items: The National Natural Science Foundation of China (No. 61772404), Shaanxi Province Key Industrial Innovation Chain (Group)-Industrial Field Project (No. 2020ZDLGY08-08), The National Natural Science Foundation of China (No. U1836203)

球站互联互通,采用星上处理和星上路由交换等技术,实施各种信息的实时获取、存储、融合和分发。现阶段我国天地一体化信息网络采用多层次天基信息网络,其中,低地球轨道(Low Earth Orbit, LEO)卫星通信网络由于其链路损耗小、星地时延小、卫星成本低、部署灵活等优势,受到研究人员的青睐,被广泛应用于卫星网络的建设中。

天地一体化信息网络具有典型的大时空尺度特性,网络拓扑结构高度异构且动态复杂、传输时延大、网络资源有限。除此之外,其空间节点计算能力和存储能力有限,对组网过程中的协议或算法的复杂度要求严格。天地一体化信息网络还面临蓄意攻击与破坏等安全威胁,易受到敌方窃听、假冒、信息重放等攻击。因此,为了保障合法用户的权益和隐私,维护天地一体化信息网络的安全,用户和卫星网络需要实现实体身份双向认证后,再获取网络服务。首先,天地一体化信息网络结构复杂,且其建设中需要不断地扩展补充,接入随意性大,需要安全可靠的实体身份认证协议。其次,一方面,LEO卫星网络一般部署海量卫星以实现全球无缝覆盖,故在卫星节点密集的环境中进行网内信息广播时,有可能产生物理环路,严重时会导致区域网络中断;另一方面,由于通信链路易受干扰,容易造成通信中断。如果每次都执行完整的一套初始接入认证,耗时耗力,故需要设计安全快速的通信恢复认证机制。最后,低轨道卫星和地球处于相对运动中,通信链路不稳定,且卫星覆盖范围在不断变化,用户需要实时进行信号覆盖检测,选择新的卫星接入点以保证通信服务的高质量 and 连续性。

由于天地一体化信息网络的战略地位和优越性,其建设得到了国内外越来越多的关注,很多学者团队针对天地一体化信息网络提出了大量的安全认证方案。1996年,CRUICKSHANK^[1]利用公私钥体系完成用户与卫星网络的互相认证和密钥协商,保障前向安全。但是,该方案没有实现用户终端身份的匿名性,可能造成用户的身份信息泄露,从而引发一系列攻击;它使用数字签名,不适合计算能力受限的用户和卫星网络。针对CRUICKSHANK方案的问题,2003年,HWANG等^[2]提出了针对移动卫星通信系统的移动用户匿名认证和数据加密新方案,该方案可以抵抗重放攻击,降低了计算开销。但是,该方案不具备前向安全性,同时会遭受密码猜测攻击。传统网络的用户漫游认证需要向用户归属域请求身份信息,增加了认证开销与通信负担。2010年,YANG等^[3]提出了两方参与下的漫游方案,避免传统三方认证的烦琐操作,引入了用户撤销机制,支持强的两方

漫游的挑战性问题,但签名算法的复杂性带来了较大的开销。2012年,针对多访问点的无缝切换场景,HE等^[4]提出的方案采用假名隐私保护技术、PairHand配对技术和批量签名技术,提高切换方案的效率,但由于涉及公钥密码和大量双线性映射操作,方案计算开销大,且不具备前向安全性。2014年,YAN等^[5]结合北斗卫星导航系统提供的短消息通信和星载时钟高度一致的特点,实现了域间漫游认证和用户身份匿名保护,减少了归属域认证中心的开销,但通过全球认证中心来分发票据密钥,并没有减少总体计算开销,且增加了票据管理压力。2016年,JIANG等^[6]提出了一种高效、匿名的批量认证方案,该方案基于HMAC的公钥基础设施来完成对用户的接入认证,引入大量开销。针对身份的无线认证和密钥协商问题,BAO等^[7]基于椭圆曲线密码体制进行认证,认证过程清晰简单,由于针对的是地面无线网络设计,计算开销较大。

4G与5G的快速普及和发展带动了安全认证机制的研究。在LTE-A网络下,3GPP提出了一个切换认证方案^[8],但是该方案存在多个安全漏洞,包括中间人攻击、重定向攻击、拒绝服务(Denial of Service, DoS)攻击和身份隐私泄露等^[9]。2007年,KIM等^[10]提出了一个基于身份加密的漫游方案,此方案降低了通信开销,涉及大量双线性映射操作,计算开销大。2012年,CHOI等^[11]提出了基于代理签名的切换认证方案,但是不能提供足够的前向安全和后向安全性。2018年,QIU等^[12]提出了一种改进的基于代理签名的切换认证方案,此方案解决了安全性问题,但是通信开销大。5G标准中,3GPP SA3提出了一个切换认证协议^[13]试图解决以上问题,但仍然存在一些安全漏洞,例如可追溯性攻击等^[14]。

通过上述分析,现阶段卫星认证技术存在的问题和缺陷如下。

(1) 现阶段接入认证技术方案大多实现了用户匿名认证,但卫星和用户终端资源和计算能力受限,如果采用公钥密码体制或椭圆曲线点乘算法等计算开销较大的密码算法,认证时间长,耗能快。特别是未来趋势将实现多样化终端接入,对于要求低能耗的物联网(Internet of Things, IoT)设备来讲更需要轻量级的算法来延长设备单次使用时间。

(2) 现阶段的认证方案大多考虑初始接入认证和用户切换场景,较少考虑卫星链路断开后的重连过程。在这种场景下,重复执行初始接入认证过程烦琐,造成计算和通信资源浪费,增加卫星和地面站负担。

(3) 在卫星切换场景下,更新会话密钥过程存在安全和性能相关问题,且没有考虑卫星轨道可预测的问题,如果提前计算部分认证开销,可优化认证方案。

2 系统模型、安全需求 and 设计思路

2.1 系统模型

本文主要研究天地一体化信息网络中的安全接入、通信恢复和卫星切换认证问题。这一过程主要考虑以下实体：用户设备（User Equipment, UE）、LEO卫星网络以及网络控制中心（Network Control Center, NCC），系统架构如图1所示。

（1）UE是在地面和卫星进行通信的终端。在其归属域NCC上注册，通过星地链路接入LEO卫星网络获取通信服务。

（2）LEO卫星网络由若干颗在地球低轨道运行的LEO卫星构成，具有有限的计算能力和存储能力。LEO卫星是UE和NCC间的中继节点，可进行UE与NCC间的数据通信和传输，相邻的LEO卫星间可以通过星间链路进行信息传递。

（3）NCC是卫星网络的地面控制中心，负责计算、验证UE身份等需要较多计算和存储能力的功能。

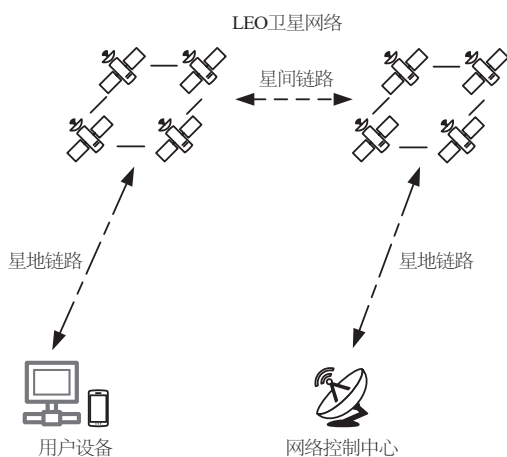


图1 系统架构

2.2 安全需求

根据所述网络架构，结合安全协议形式化分析研究的Dolev-Yao模型，天地一体化信息网络的接入认证协议有如下安全需求。

（1）用户匿名。UE的真实身份只有NCC知晓，对其余角色使用假名，即其余网络节点在不获得用户真实身份的情况下，仍能为合法用户提供通信服务。此外，同一用户在多次获取网络服务时所使用的假名应各不相同，且不具有关联性。

（2）双向认证。NCC需要认证UE的身份，确认其具有接入网络的资格。同时UE也需要认证NCC的身份，

防止接入虚假服务网络，避免造成隐私泄露等问题。

（3）密钥协商。在初始认证结束之后，UE应和NCC协商会话密钥，用于后续通信的认证和加密。当发起卫星切换时，也应协商新的会话密钥。

（4）抵抗拒绝服务攻击。卫星的资源有限，当攻击者发起大量恶意接入请求时极易耗尽网络资源，造成服务网络瘫痪。故认证方案需要具有抵抗拒绝服务攻击的能力。

（5）抵抗重放攻击。攻击者可以通过窃听或截获等手段捕获合法的消息再重放，以欺骗认证方，干扰认证过程。故认证方案应该采取合适的措施应对重放攻击。目前，应对重放攻击的措施主要分为添加时间戳、序列号或完成挑战响应机制。

2.3 设计思路

方案主要包括用户注册、初始接入、通信恢复和卫星切换4个阶段，整体认证流程如图2所示。

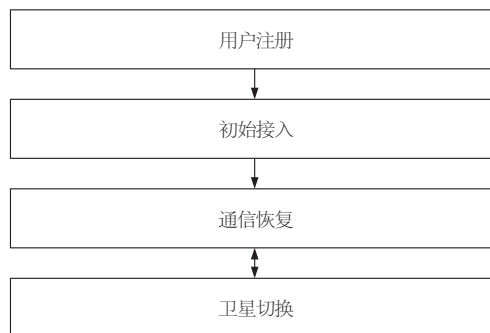


图2 整体认证流程

在卫星发射升空前，UE首先需要在归属域完成注册，包括离线生成用户身份、长期共享密钥等。同时，在此过程中，UE使用自己的身份标识（User Identification, UID）注册并获取NCC返回的临时身份TID。此TID每次认证成功后会刷新，确保安全性。在初始接入认证阶段，即UE第一次接入卫星网络时，主要使用哈希函数和异或来进行运算，通过引入时间戳、消息鉴别码、随机数和RES确保安全，并产生会话密钥。

UE成功接入卫星网络后，由于实际环境中天地链路的不稳定性，引入了UE和LEO卫星网络连接断开后的通信恢复阶段，并产生新的会话密钥；考虑到实际环境中卫星在不断运动中存在UE切换卫星接入点等问题，引入了卫星切换阶段。在NCC的协助下，原卫星和新卫星产生新的会话密钥并返回给UE。

3 方案设计

3.1 用户注册

实现用户设备注册入网，离线注册终端初始接入认证密钥等，为进一步认证做好准备，用户注册流程如图3所示，具体过程如下。

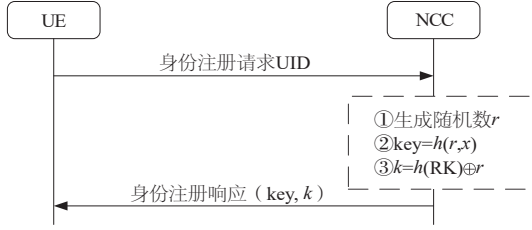


图3 用户注册流程

3.2 初始接入

针对卫星网络星地时延较大、网络拓扑结构动态变化以及星载资源受限等特点，本文提出了一种安全的轻量级接入认证协议，如图4所示。基于对称密码实现通信双方实体身份认证，结合计算量较小的哈希和异或操作减少了通信过程中的计算开销，具体过程如下。

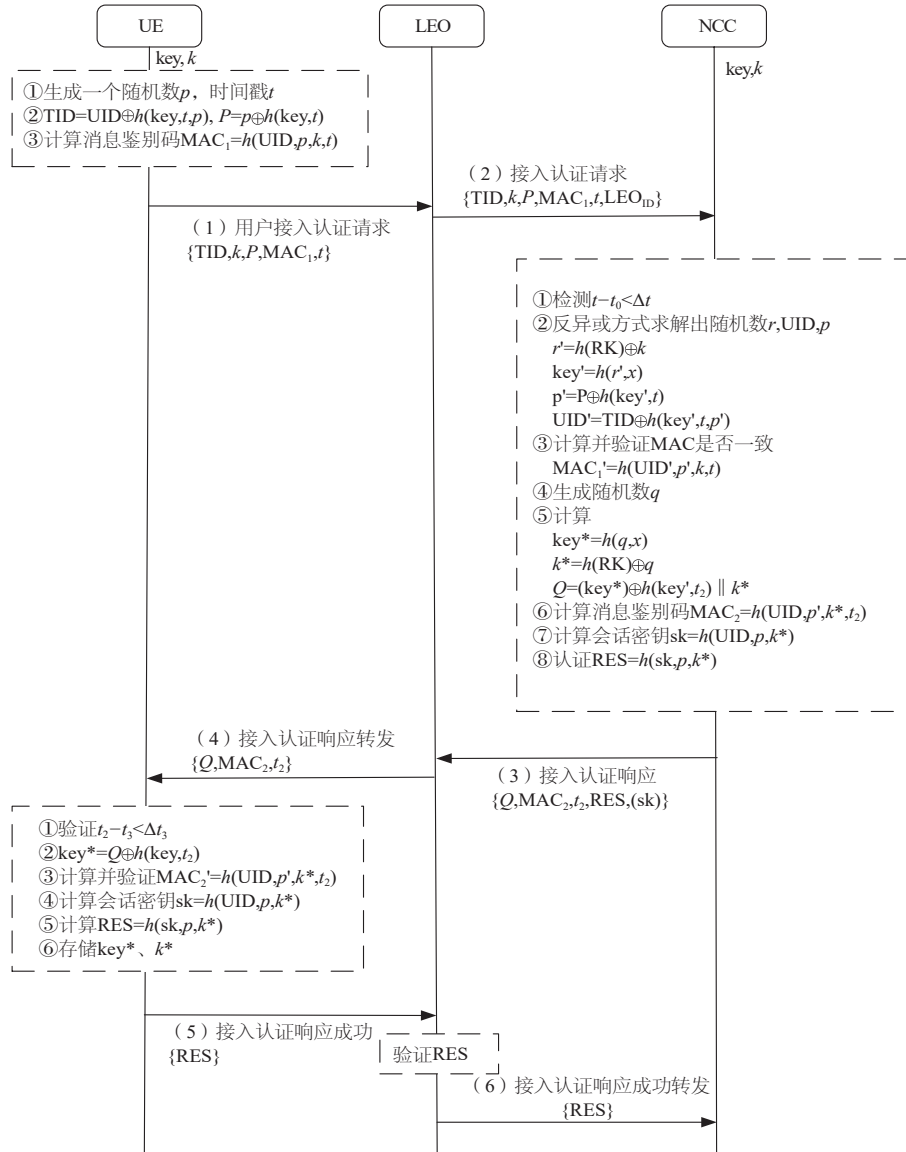


图4 安全的轻量级初始接入认证

注1：本文中(·)表示安全信道传输的内容，{}表示公共信道。

(1) UE首次接入卫星网络时,生成一个随机数 p ,计算 $TID=UID \oplus h(\text{key}, t, p)$ 、 $P=p \oplus h(\text{key}, t)$,计算消息认证码 $MAC_1=h(UID, p, k, t)$,其中, t 为当前时间戳, key 和 k 在注册过程中获得。UE将用户接入认证请求消息 $\{TID, k, p, MAC_1, t\}$ 发送给LEO卫星网络。

(2) LEO卫星网络收到消息后,在消息上附加其ID,并将信息发送给NCC。

(3) NCC收到消息后,首先检测时间戳 $t-t_0$ 是否在允许区间内,其中 t_0 为NCC收到消息时的时间。若在允许时间范围内,NCC由反异或算法计算出随机数 $r'=h(RK) \oplus k$,计算 $p'=P \oplus h(h(r', x), t)$,然后由随机数 r' 和 p' 解出UE的真实身份标识 $UID'=TID \oplus h(h(r', x), t, p')$ 。计算并验证 $MAC_1'=h(UID', p', k, t)$ 是否与收到的 MAC_1 相等,若相等则进入下一步。即NCC生成随机数 q ,计算 $\text{key}^*=h(q, x)$,新的 $k^*=h(RK) \oplus q$,计算 $Q=(\text{key}^*) \oplus h(h(r', x), t_2) \parallel k^*$,计算消息鉴别码 $MAC_2=h(UID', p', k^*, t_2)$,其中 t_2 为当前时间戳,计算会话密钥以及认证响应。最后,NCC将 $\{Q, MAC_2, t_2, RES, (sk)\}$ 发送给LEO卫星网络,其中 sk 通过安全信道发送。

(4) LEO卫星网络收到信息后,本地保存 RES 、 sk ,然后将 $\{Q, MAC_2, t_2\}$ 转发给UE。

(5) UE收到消息后,首先检查时间戳 t_2-t_3 是否在允许区间内,其中 t_3 为UE收到消息时的时间。如果时间差不在允许区间内则结束会话;如果在允许区间内则进行下面的过程。即UE利用反异或算法计算出 $\text{key}^*=h(\text{key}, t_2) \oplus Q$, $MAC_2'=h(UID, p', k^*, t_2)$ 并且验证 MAC_2' 是否与接收到的 MAC_2 一致。若不一致则结束会话;若一致则计算会话密钥 $sk=h(UID, p, k^*)$ 和响应 $RES=h(sk, p, k^*)$,并将 RES 发送给卫星网络LEO,UE存储 key^* , k^* 用于可能的再次认证。

(6) LEO卫星网络收到信息后,本地验证收到的 RES' 与本地存储的 RES 是否相等。若相等,则将消息转发给NCC;否则,向NCC和UE报告认证失败。

(7) NCC收到消息后,验证 $RES=h(sk, p, k^*)$ 。若验证失败,结束会话;若验证成功,认证过程完成。此时, sk 作为卫星与UE通信的会话密钥。

3.3 通信恢复

针对卫星网络通信中断链问题,本文基于断链前会话密钥提出了一种通信恢复认证方案。如图5所示,认证过程简单、计算量较初始接入认证小,并完成新的会话密钥协商。一方面,此过程减少了卫星与NCC的交互次数,减轻NCC负担;另一方面,断续重连可以避免频繁发起初始认证耗费大量资源的问题。具体过程如下。

(1) UE生成随机数 m ,计算 $M=h(sk, t_1) \oplus m$ 向LEO卫星网络发送连接恢复请求消息 $\{TID, M, t_1\}$,其中 t_1 为当前时间戳。

(2) 卫星收到消息后,首先检查时间戳 t_1 的有效性;然后求解出 $m'=M \oplus h(sk, t_1)$;随后,LEO卫星网络生成随机数 n ,计算 $N=h(sk, t_2) \oplus n$, $MAC=h(TID, m', n, t_2)$,将 $\{N, MAC, t_2\}$ 发送给UE,其中 t_2 是当前时间戳。

(3) UE收到消息后,检查时间戳 t_2 的有效性,若有效求解出 $n'=N \oplus h(sk, t_2)$,验证 MAC 是否正确。若验证失败结束会话;若验证成功,计算新的会话密钥 $sk_2=h(TID, m, n')$,计算 $RES_2=h(sk_2, m, n')$,并将 RES_2 发送给卫星。

(4) 卫星收到消息后计算 $sk_2=h(TID, m', n)$,验证 $RES_2=h(sk_2, m', n)$,若验证失败则结束会话, sk_2 作为卫星与UE通信新的会话密钥。

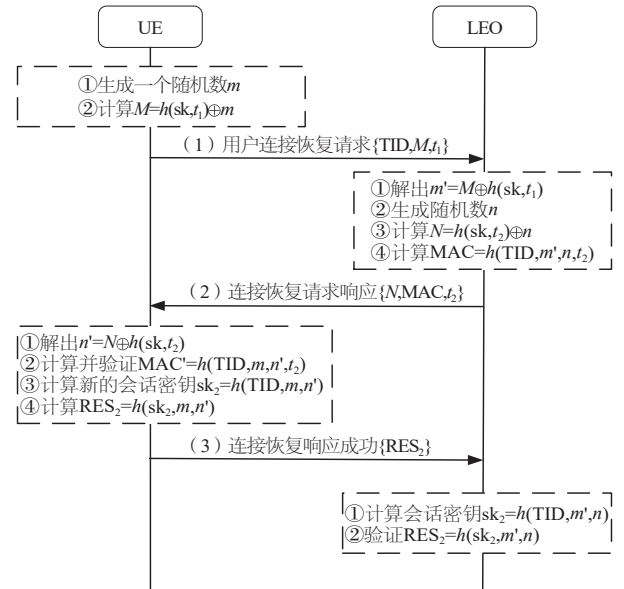


图5 通信恢复认证方案

3.4 卫星切换

针对卫星节点高速移动的身份认证问题,本文基于随机数和哈希操作设计了一种卫星无缝切换和快速密钥协商方案,如图6所示。UE可以在真实切换发生前发起预切换,从而在切换发生时可以快速完成切换,确保真实的切换认证时延很短,为UE提供较为平滑的通信体验,同时尽可能减少系统开销。具体过程如下。

(1) 当UE监测到原卫星 LEO_1 即将离开其可接收信号区时,UE向 LEO_1 发送预切换请求 TID 以及UE的位置信息, LEO_1 根据UE的位置信息以及卫星轨迹信息决策UE即将接入的下一个卫星 LEO_2 。若 LEO_1 无法决策出UE即将接入的下一个卫星,则将UE的位置信息发送给

NCC；NCC根据轨迹预测为UE选择新的接入卫星，将新卫星LEO₂的ID₂与轨道信息发送给原卫星LEO₁。

(2) 原卫星LEO₁产生随机数 s_1 ，计算 $K_1=h(s_1,sk)$ ，其中 sk 为当前卫星的会话密钥，原卫星LEO₁通过卫星间已经提前建立好的安全通道向新卫星LEO₂发送 $\{TID,(K_1)\}$ 。

(3) 新卫星LEO₂收到消息后，生成随机数 s_2 ，计算新的会话密钥 $sk'=h(K_1,s_2)$ ，并将 s_2 发回原卫星LEO₁。

(4) 原卫星LEO₁将 $\{s_1,s_2\}$ 发给UE。

(5) UE收到消息后，计算 $sk'=h(h(s_1,sk),s_2)$ 。此 sk' 作为UE和新卫星LEO₂通信的会话密钥。

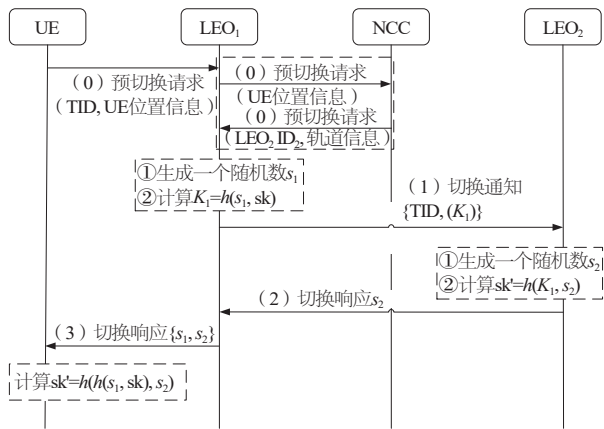


图6 卫星无缝切换和快速密钥协商方案

4 安全性分析

以下分别采用非形式化和形式化安全分析来证明本文提出方案的安全性。

4.1 非形式化安全分析

下面采用非形式化安全分析证明本文提出方案的安全性。

(1) 用户匿名性：初始接入认证过程，用户终端根据共享认证密钥生成临时身份标识 $TID=UID \oplus h(key, t, p)$ ，其中， key 是UE和NCC间的共享密钥、 t 是时间戳、 p 是随机数，并且，每次认证结束后会更新TID，攻击者不具备密钥 key ，无法从TID中获取用户真实身份UID，也不能伪造用户身份。

(2) 相互认证：初始接入认证过程，用户通过比较接收到的消息验证码 MAC_2 和本地生成的 MAC_2' 是否相等来鉴别NCC的实体身份；同时NCC通过比较收到的 MAC_1 和本地生成的 MAC_1' 是否相等来鉴别用户的实体身份，实现双向身份认证。

(3) 防止用户假冒攻击：发起认证请求时，合法UE需要向NCC发送 $\{TID, k, P, MAC_1, t\}$ ，而攻击者不知道用户和

NCC间的注册密钥 k 以及用户的真实身份标识UID，无法生成合法的MAC，本文提出的方案能够抵御用户假冒攻击。

(4) 防止服务器假冒攻击：初始接入认证过程，假冒NCC需要发送的认证响应消息 $\{Q, MAC_2, t_2, RES, (sk)\}$ ，而 MAC_2 和 Q 是基于UE和NCC间共享密钥生成的，攻击者无法获取共享密钥解密的随机数 p 、 q ，无法生成合法的响应消息，本文提出的方案能够抵抗服务器假冒攻击。

(5) 抵御拒绝服务攻击：本文提出的方案中，NCC通过哈希和异或算法获取用户身份、共享认证密钥等信息来生成消息验证码，以验证UE身份，无须向数据库请求用户身份信息，如 $\{UID, key, k\}$ ；避免频繁请求数据库造成资源耗尽的问题。即使大量非法用户恶意接入，也能在短时间内甄别出合法用户请求，抵御拒绝服务攻击。

(6) 抵御重放攻击：初始接入认证过程中，在UE发送的认证请求消息 $\{TID, k, P, MAC_1, t\}$ 和NCC发送的认证响应消息 $\{Q, MAC_2, t_2, RES, (sk)\}$ 中加入时间戳，保证消息的不可重放性。同时，使用时间戳和随机数生成消息验证码，敌手无法篡改和重放消息。通信恢复认证过程类似。故本文提出的方案能够抵御重放攻击。

4.2 Scyther形式化安全分析

本文涉及用户注册、初始接入、通信恢复和卫星切换4个阶段，本小节将用户注册和初始接入认证合并为一个阶段进行形式化分析，通信恢复阶段单独进行形式化分析。由于卫星切换部分只是通过原卫星安全传递协商密钥，故不进行形式化安全分析。

使用Scyther工具对本小节协议进行形式化分析^[16]，首先需要将本小节协议转化为形式化语义，之后和安全属性结合，最后运行Scyther工具输出分析结果。由于Scyther本身采用的是黑盒验证思想，各个角色（Role）从自己的角度来观察是否能够满足安全目标和安全属性。

Scyther内置哈希操作、对称加密及解密操作等。首先，需要声明哈希函数；其次，声明协议名和角色集；最后，角色集声明变量、定义收发消息事件和声明安全属性。若声明的安全属性不被满足，则可能存在攻击路径。模型化结束后，Scyther工具自动输出验证结果。验证结果有两种类型：如果安全属性满足，输出verified；反之，则输出falsified。本小节需要验证的两个过程分别涉及两方，即NCC和UE，或LEO和UE。本文对通信双方发送和接收的每条消息声明了以下安全属性，分别为Secret、Alive、Weakagree、Niagree和Nisynch，协议过程、运行结果与分析如下。

(1) 用户注册和初始接入认证阶段

由于提出的方案采用哈希操作和对称密码加解密，

故首先需要提前声明哈希函数；然后，定义协议名和角色集。LEO在此过程中充当中继节点，故省略它转发消息的过程。具体设置如下：

```
hashfunction  $h$ ;
protocol authentication( UE, NCC){
  role UE {}
  role NCC {}
}
```

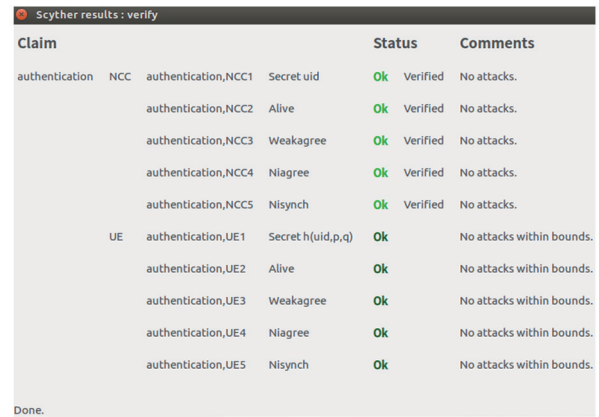
此阶段UE生成并发送包含MAC₁在内的认证请求，生成会话密钥sk，接收验证MAC₂、RES；NCC接收验证MAC₁，生成会话密钥sk，生成并发送包含MAC₂、RES在内的认证响应。其中，需要保证sk、uid的保密性。具体设置如下：

```
role UE
{
  fresh  $t, p$ , uid: Nonce;
  var  $x, r, t_2, q$ : Nonce;
  send_00 (UE, NCC, {uid}  $k$ (UE, NCC));
  rcv_0 (NCC, UE, TID,  $k$ );
  macro  $P = \{p\} h(r, x)$ ;
  macro  $MAC_1 = h(uid, p, t)$ ;
  send_1 (UE, NCC, TID,  $k, P, MAC_1$ );
  rcv_2 (NCC, UE, Q,  $MAC_2, t_2$ );
  macro  $sk = h(uid, p, q)$ ;
  macro  $RES = h(sk, p, q)$ ;
  send_3 (UE, NCC, RES);
  claim (UE, Secret, sk);
  claim (UE, Alive);
  claim (UE, Weakagree);
  claim (UE, Niagree);
  claim (UE, Nisynch);
}

role NCC
{
  fresh  $x, r, q$ : Nonce;
  fresh  $t_2$ : Nonce;
  var uid,  $t, p$ : Nonce;
  rcv_00 (UE, NCC, {uid}  $k$ (UE, NCC));
  macro TID = { $h(r, x)$ } uid;
  macro  $k = \{r\} h(TID, x)$ ;
  send_0 (NCC, UE, TID,  $k$ );
  macro  $P = \{p\} h(r, x)$ ;
  macro  $MAC_1 = h(uid, p, t)$ ;
  rcv_1 (UE, NCC, TID,  $k, P, MAC_1, t$ );
```

```
macro  $Q = \{q\} h(r, x)$ ;
macro  $MAC_2 = h(uid, p, q, t_2)$ ;
send_2 (NCC, UE, Q,  $MAC_2, t_2$ );
macro  $sk = h(uid, p, q)$ ;
macro  $RES = h(sk, p, q)$ ;
rcv_3 (UE, NCC, RES);
claim (NCC, Secret, uid);
claim (NCC, Alive);
claim (NCC, Weakagree);
claim (NCC, Niagree);
claim (NCC, Nisynch);
}
```

图7显示了用户注册与初始接入认证阶段Scyther仿真结果。从图7可知，NCC通信的内容中，声明的Secret、Alive、Weakagree、Niagree和Nisynch属性在状态空间界限外或者内部都没有发现攻击；UE通信的内容中，声明的Secret、Alive、Weakagree、Niagree和Nisynch属性在限制范围内没有找到攻击。因此，用户注册和初始接入认证阶段可以防御重放攻击、中间人攻击等恶意攻击，能够实现相互身份认证和机密数据的保护。



Claim	Status	Comments
authentication, NCC authentication, NCC1 Secret uid	Ok Verified	No attacks.
authentication, NCC2 Alive	Ok Verified	No attacks.
authentication, NCC3 Weakagree	Ok Verified	No attacks.
authentication, NCC4 Niagree	Ok Verified	No attacks.
authentication, NCC5 Nisynch	Ok Verified	No attacks.
UE authentication, UE1 Secret $h(uid, p, q)$	Ok	No attacks within bounds.
authentication, UE2 Alive	Ok	No attacks within bounds.
authentication, UE3 Weakagree	Ok	No attacks within bounds.
authentication, UE4 Niagree	Ok	No attacks within bounds.
authentication, UE5 Nisynch	Ok	No attacks within bounds.

图7 用户注册与初始接入认证阶段Scyther仿真结果

(2) 通信恢复认证阶段

声明哈希函数，定义协议名和角色集。具体设置如下：

```
hashfunction  $h$ ;
protocol recovery( UE, LEO){
  role UE {}
  role LEO {}
}
```

此阶段UE生成并发送包含M在内的认证请求，生成新的会话密钥sk₂，接收验证MAC，发送认证确认响应RES；LEO接收获得M，生成会话密钥sk₂，生成并发送

MAC在内的认证响应,验证RES。具体设置如下:

```

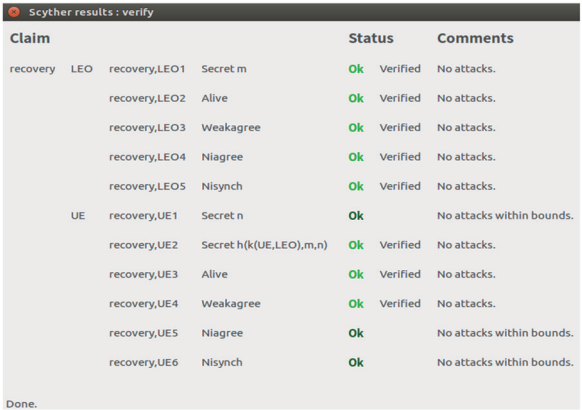
role UE
{
  fresh  $m$ : Nonce;
  var  $n$ : Nonce;
  send_1 (UE, LEO,  $\{m\}k(UE, LEO)$ );
  rcv_2 (LEO, UE,  $\{n\}k(UE, LEO), MAC$ );
  macro  $sk_2 = h(k(UE, LEO), m, n)$ ;
  send_3 (UE, LEO,  $h(sk_2, m, n)$ );
  claim (UE, Secret,  $n$ );
  claim (UE, Secret,  $sk_2$ );
  claim (UE, Alive);
  claim (UE, Weakagree);
  claim (UE, Niagree);
  claim (UE, Nisynch);
}

role LEO
{
  fresh  $n$ : Nonce;
  var  $m$ : Nonce;
  rcv_1 (UE, LEO,  $\{m\}k(UE, LEO)$ );
  macro  $MAC = h(m, n)$ ;
  send_2 (LEO, UE,  $\{n\}k(UE, LEO), MAC$ );
  macro  $sk_2 = h(k(UE, LEO), m, n)$ ;
  rcv_3 (UE, LEO,  $h(sk_2, m, n)$ );
  claim (LEO, Secret,  $m$ );
  claim (LEO, Alive);
  claim (LEO, Weakagree);
  claim (LEO, Niagree);
  claim (LEO, Nisynch);
}

```

图8显示了通信恢复认证阶段Scyther仿真结果。从图8可知,LEO卫星网络通信的内容中,声明的Secret、Alive、Weakagree、Niagree和Nisynch属性在状态空间界限外或者内部都没有发现攻击;UE通信的内容中,声明的Secret、Niagree和Nisynch属性在状态空间界限外或者内部都没有发现攻击,且声明的Secret、Alive、Weakagree属性在限制范围内没有找到攻击。因此,通信恢复阶段可以防御重放攻击、中间人攻击等恶意攻击,能够实现相互身份认证和机密数据的保护。

综上,最终分析结果表明,Scyther工具无法找到针对本文提出的协议的任何攻击,协议能够保证通信各方的秘密信息安全,能够抵御重放攻击、中间人攻击等恶意攻击,能够实现相互身份认证和机密数据的保护,证明了本小节协议的安全性,可保证通信安全。



Claim	Status	Comments
recovery, LEO recovery, LEO1 Secret m	Ok Verified	No attacks.
recovery, LEO2 Alive	Ok Verified	No attacks.
recovery, LEO3 Weakagree	Ok Verified	No attacks.
recovery, LEO4 Niagree	Ok Verified	No attacks.
recovery, LEO5 Nisynch	Ok Verified	No attacks.
UE recovery, UE1 Secret n	Ok	No attacks within bounds.
recovery, UE2 Secret $h(k(UE, LEO), m, n)$	Ok Verified	No attacks.
recovery, UE3 Alive	Ok Verified	No attacks.
recovery, UE4 Weakagree	Ok Verified	No attacks.
recovery, UE5 Niagree	Ok	No attacks within bounds.
recovery, UE6 Nisynch	Ok	No attacks within bounds.

Done.

图8 通信恢复认证阶段Scyther仿真结果

5 性能分析

计算开销、带宽开销和信令开销对于卫星认证协议至关重要,是用来衡量一个方案是否高效的方式。本节分别评估和对比了本文提出方案与其他认证流程较为相似的方案^[17-20]的信令开销、计算开销和带宽开销。

5.1 信令开销

在信令开销上,本文假定SG (Satellite-Ground) 代表一次星地链路通信,SS (Satellite-Satellite) 代表一次星间链路通信。各协议的信令开销比较见表1。每完成一次双向身份认证,参考文献[17-19]的方案需要3次星地链路信令,但是参考文献[20]的方案和本文提出的初始接入认证过程额外进行了一次身份认证结果确认的过程,故进行了6次星地信令交互过程,相当于完成4次握手,保障认证过程更加安全。对于通信恢复认证过程,由于NCC不参与认证过程,因此,只需要3次信令消息。在卫星切换认证中,预切换过程在真实切换发生前的空闲时段完成,信令消息不加入统计,完成一次卫星切换只需要1次星地信令消息和2次星间信令消息。

另外,在完成初始接入认证后,除非轨道变动等情况,否则更多进行通信恢复和卫星切换认证。因此,本文提出的方案实际信令开销比其余方案更小。

5.2 计算开销

认证过程中涉及异或运算、级联、单向哈希运算 T_h 、点乘 T_{pm} 和对称加解密运算 T_{ED} 。其中,异或和级联需要的执行时间较短,因此在计算开销中忽略这两类运算。其余的运算按照参考文献[21]给出的计算规则和数据, T_h 、 T_{pm} 、 T_{ED} 执行一次的时间分别为0.002 39 ms、1 ms、0.002 26 ms。表1中列出了各协议的计算开销。

表1 各协议信令开销比较

参数	参考文献[17]的方案	参考文献[18]的方案	参考文献[19]的方案	参考文献[20]的方案	初始接入	通信恢复	卫星切换
信令开销/次	4 SG	4 SG	4 SG	6 SG	6 SG	3 SG	1 SG + 2 SS
计算开销/ms	$14T_h + 17T_{pm}$	$7T_h$	$10T_h$	$12T_h + 6T_{pm} + 2T_{ED}$	$17T_h$	$10T_h$	$3T_h$
带宽开销/byte	124	68	88	188	176	84	52

图9列出了各方案随着认证次数增加计算开销的变化。由于采用计算量较小的单向哈希算法,避免点乘运算,本文方案计算开销较参考文献[17]、[20]的方案小。与参考文献[18-19]的方案相比,3.2小节描述的初始接入认证中,NCC根据本地信息重新计算用户长期密钥以及最后进行认证结果确认时增加了计算开销。但是,一方面,当大量用户通过初始接入认证接入时可以减少频繁查询数据库的时间,从而减少整体认证时间;另一方面,NCC只需要保证自己私钥是安全的即可,减轻NCC密钥管理的压力。另外,每次认证都会更新认证密钥。在初始接入认证中多了一次UE和NCC间的认证结果确认,使得认证过程更加安全。在完成初始接入认证后,除非轨道变动等情况,否则更多进行通信恢复和卫星切换认证。本文提出的通信恢复计算开销仅次于参考文献[18]的方案,本文的卫星切换方案优于其余方案。

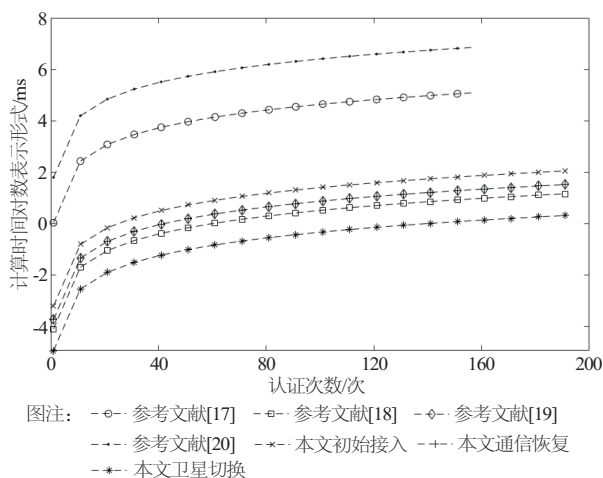


图9 各方案随着认证次数增加计算开销的变化

5.3 带宽开销

在和AES-128同等安全条件下,假设基于对称密码体制的密钥长度为128 bit,ElGamal密码体制的公钥密钥长度为3 072 bit、私钥为256 bit,椭圆曲线上的点320 bit。对

于哈希算法本文采用160 bit,加密算法采用输出数据长度为128 bit的SM4算法,最后定义随机数和身份标识的长度为128 bit,序列号、AMF标识的长度为48 bit,身份标识长度、时间戳为32 bit。表1中列出了各协议的带宽开销。

根据不同场景,本文将参考文献[17-20]的方案分为初始接入、通信恢复和卫星切换3个认证阶段进行比较。图10列出了各方案在不同认证阶段总的带宽开销情况。根据图10,3.2小节提出的初始接入认证传输会话密钥和认证结果确认增加了带宽开销。然而,初始接入认证执行次数较少,在通信恢复和卫星切换中,本文方案带宽低于参考文献[17]、[19]、[20]的方案。

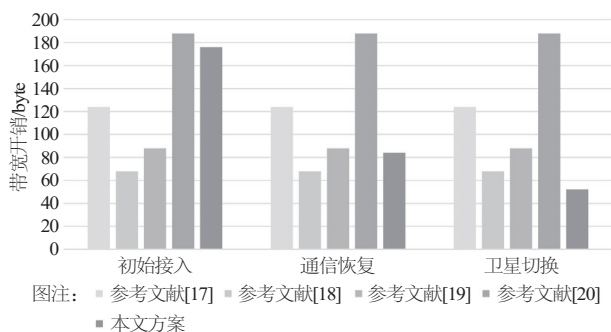


图10 各协议带宽开销比较

表2列出了各方案安全性和综合性能开销的情况。由于卫星切换部分只是通过原卫星安全传递协商密钥,故安全需求在此不做分析。由表2可以看出,在列出的所有方案中,3.4小节提出的卫星切换认证总体性能开销最小。参考文献[18-19]的方案和3.3小节提出的通信恢复认证过程的信令、计算、带宽开销较小且相近,但是参考文献[18-19]的方案没有满足要求的安全需求,不适合卫星网络认证。虽然参考文献[17]的方案在性能开销上优于3.2小节提出的初始接入认证,但是没有满足抗重放攻击和抗DoS

表2 安全性和性能分析对比

性能	初始接入	通信恢复	卫星切换	参考文献[17]的方案	参考文献[18]的方案	参考文献[19]的方案	参考文献[20]的方案
双向认证	Y	Y	-	Y	N	Y	Y
密钥协商	Y	Y	-	Y	N	Y	Y
匿名性	Y	Y	-	Y	N	Y	Y
抗重放攻击	Y	Y	-	N	N	Y	Y
抗DoS攻击	Y	Y	-	N	N	N	Y
信令开销	H	L	L	M	L	L	H
计算开销	M	M	L	H	M	M	H
带宽开销	H	L	L	M	L	L	H

说明: Y: Yes; N: No; H: High; M: Medium; L: Low; -: 不做分析

攻击。参考文献[20]的方案满足所列出的安全需求，但是由于采用椭圆曲线密码体制（Elliptic Curve Cryptosystems, ECC），计算开销较大。综上所述，在满足相同安全需求的条件下，本文提出的方案总体性能开销更小。

6 结束语

本文针对用户和移动卫星网络的场景设计了全方面、多层次的接入认证和通信保持方案，实现了用户和卫星网络双向认证，保障用户可以安全高效地接入卫星网络、获取网络服务。其中，初始接入认证保障用户在卫星网络的辅助下安全、高效地接入地面网络；通信恢复认证保障链路中断后用户可以安全快速地恢复网络服务；切换认证保障用户终端可以无缝切换卫星接入点，保证卫星网络服务的连续性。本文设计初始接入认证、通信恢复和卫星切换仅使用密码学中的异或算法和哈希算法，计算开销较少，认证效率高。由于天上设备维修困难等问题，任何一个节点的失效都不应该影响整个网络，所以未来研究方向还可以增加失效节点的更新等问题。

参考文献：

- [1] CRUICKSHANK H S. A security system for satellite networks[C]//Proceedings of Fifth International Conference on Satellite Systems for Mobile Communications and Navigation. Piscataway: IEEE Press, 1996: 187-190.
- [2] HWANG M S, YANG C C, SHIU C Y. An authentication scheme for mobile satellite communication systems[J]. ACM SIGOPS Operating Systems Review, 2003, 37(4): 42-47.
- [3] YANG G M, HUANG Q, WONG D S, et al. Universal authentication protocols for anonymous wireless communications[J]. IEEE Transactions on Wireless Communications, 2010, 9(1): 168-174.
- [4] HE D J, CHEN C, CHAN S, et al. Secure and efficient handover authentication based on bilinear pairing functions[J]. IEEE Transactions on Wireless Communications, 2012, 11(1): 48-53.
- [5] YAN J, LU Y, LIU Y L, et al. Research on Beidou-based inter-domain identity authentication for mobile object[C]//Proceedings of 2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA). Piscataway: IEEE Press, 2014: 923-926.
- [6] JIANG S R, ZHU X Y, WANG L M. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2193-2204.
- [7] BAO Q R, HOU M B, CHOO K K R. A one-pass identity-based authentication and key agreement protocol for wireless roaming[C]//Proceedings of 2016 Sixth International Conference on Information Science and Technology (ICIST). Piscataway: IEEE Press, 2016: 443-447.
- [8] 3rd Generation Partnership Project. Technical specification group services and system aspects, General Packet Radio Service(GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (EUTRAN) access (Rel 15): 3GPP TS 23.401 v15.3.0[S]. 2018.
- [9] CAO J, MA M D, LI H, et al. A survey on security aspects for LTE and LTE-A networks[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1): 283-302.
- [10] KIM Y, REN W, JO J Y, et al. SFRIC: a secure fast roaming scheme in wireless LAN using ID-based cryptography[C]//Proceedings of 2007 IEEE International Conference on Communications. Piscataway: IEEE Press, 2007: 1570-1575.
- [11] CHOI J, JUNG S. A handover authentication using credentials based on chameleon hashing[J]. IEEE Communications Letters, 2010, 14(1): 54-56.
- [12] QIU Y, MA M D, WANG X L. A proxy signature-based handover authentication scheme for LTE wireless networks[J]. Journal of Network and Computer Applications, 2017, 83: 63-71.
- [13] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Rel 15): 3GPP TS 33.501 v15.3.1[S]. 2018.
- [14] CREMERS C, MAUW S. Operational semantics[M]. Semantics and Verification of Security Protocols. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.
- [15] 侯峻峰. 安全协议形式化验证方法和安全协议设计研究[D]. 北京: 清华大学, 2004.
- [16] HOU J F. Research on formal verification and design of security protocols[D]. Beijing: Tsinghua University, 2004.
- [17] 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.
- [18] 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.
- [19] ALTAF I, ARSLAN A M, MAHMOOD K, et al. A novel authentication and key-agreement scheme for satellite communication network[J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(7): e3894.
- [20] CHANG C C, CHENG T F, WU H L. An authentication and key agreement protocol for satellite communications[J]. International Journal of Communication Systems, 2014, 27(10): 1994-2006.
- [21] ZHANG Y Y, CHEN J H, HUANG B J. An improved authentication scheme for mobile satellite communication systems[J]. International Journal of Satellite Communications and

Networking, 2015, 33(2): 135-146.

- [20] QI M P, CHEN J H, CHEN Y T. A secure authentication with key agreement scheme using ECC for satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2019, 37(3): 234-244.
- [21] 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]



石小平（1997-），女，西安电子科技大学网络与信息安全学院硕士生，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研究等。



马如慧（1991-），女，博士，西安电子科技大学网络与信息安全学院讲师，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研究等。



曹进（1985-），男，博士，西安电子科技大学网络与信息安全学院教授、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。



李晖（1968-），男，博士，西安电子科技大学网络与信息安全学院教授、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。



陈李兰（1997-），女，西安电子科技大学网络与信息安全学院硕士生，主要研究方向为天地一体化信息网络终端接入安全等。



李凤华（1966-），男，博士，中国科学院信息工程研究所教授、博士生导师，主要研究方向为网络与系统安全、隐私计算、密码应用等。