# 面向软件定义卫星网络的协同接入认证机制

宋 晨[1,2], 王利明[1], 徐 震[1], 李宏佳[1]

[1] 中国科学院信息工程研究所第五研究室 北京中国 100093
[2] 中国科学院大学网络空间安全学院 北京中国 100049

**摘要** 接入认证是保障卫星网络安全的重要基础技术之一, 一直为传统卫星网络安全领域的研究热点, 但在新兴的软件定义卫星网络中的相关研究尚处于“襁褓”阶段。本文面向软件定义卫星网络提出了一种协同接入认证机制, 其目标为: 将安全技术和软件定义技术有机融合, 在保证基本安全接入认证功能基础上, 抵御卫星网络接入认证拒绝服攻击, 规避由于切换认证中断导致的服务访问质量问题。协同接入认证机制设计中的主要贡献主要包括: 协同接入认证模型和空间拓扑动态变化高容忍的接入认证协议两部分。其中, 为了抵御接入认证拒绝服务攻击, 协同接入认证模型设计为以地面合法端用户设备身份作为序参量, 协同软件定义卫星网络管理面、控制面与转发面, 仅上报注册的合法端用户设备的接入认证请求, 减少接入认证暴露的攻击面; 为了提升服务访问的连续性, 空间拓扑动态变化高容忍的接入认证协议则基于椭圆曲线无证书算法, 通过主动更新预接入和接入认证阶段的控制面转发控制参数, 使合法端用户设备的服务访问对切换无感知, 降低重认证次数。通过安全性分析, 本文证明了所提出的接入认证机制不仅能够满足安全性需求, 并且与典型认证方法相比, 在抵御接入认证抗拒绝服务攻击和保障访问连续性等方面具有优势; 进一步, 通过数值仿真, 验证了所提接入认证机制不仅可有效降低重认证次数, 并且可达到毫秒级的认证算法计算效率。

**关键词** 软件定义卫星网络; 接入认证; 椭圆曲线; 无证书
**中图法分类号** TN927.2 DOI 号 10.19363/J.cnki.cn10-1380/tn.2023.03.09

# A Synergetic Authentication Scheme for Software Defined Satellite Network

SONG Chen[1,2], WANG Liming[1], XU Zhen[1], LI Hongjia[1]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

**Abstract** The access authentication is one of key techniques to guarantee the security of satellite networks. The researches on access authentication for classical satellite networks have thus gained great momentum over the past few decades, while the researches on access authentication for the promising Software-Defined Satellite Network (SDSN) are still in its infancy. In this paper, we propose a synergetic authentication scheme for the SDSN, including a synergetic authentication model and an access authentication protocol with highly tolerant capability for topological dynamics in SDSN. Merging security technique and Software-Defined technique together can not only endorse the access authentication for SDSN, but also inherently resist to the DoS attacks in the process of access authentication in SDSN. Moreover, this scheme helps avoiding service access interruption which is caused by handover among different satellites. In the synergetic authentication model, to reduce the attack surface of the access authentication service, the identity of each legitimate Satellite Terminal (ST) is used as the order parameter; based on this parameter and the coordination of the management plane, the control plane and the data plane of SDSN, we filter and only forward the legitimate STs' access authentication requests to the access authentication service. In the access authentication protocol, certificateless public key cryptography based on elliptical curve cryptography (ECC) is adopted; and, to improve the service continuity of STs during handover, we proactively update the forwarding-and-control parameter to reduce the handover latency and the interruption time of STs' ongoing services. By using the security analysis, we prove that proposed scheme can meet the basic security requirements of access authentication, thwart the access authentication DoS attacks and improve the service continuity of handover STs. Moreover, through numerically simulations, we demonstrate that the proposed scheme can effectively reduce the number of re-authentications, and the computation of the access authentication can be achieved within milliseconds.

**Key words** software defined satellite network; access authentication; elliptical curve; certificateless

---

**通讯作者:** 王利明, 博士, 正高级工程师, Email:wangliming@iie.ac.cn。
本课题得到中科院重点部署项目(No. ZDRW-KT-2016-02)课题“天基信息安全共享与服务机制研究”、国家重点研发计划项目(No. 2017YFB1010004)的资助。
收稿日期: 2020-02-14; 修改日期: 2020-06-12; 定稿日期: 2022-12-20

## 1 概述

随着航天和信息技术的蓬勃发展, 空间网络的发展经历了单星模式、星座模式、网络化模式, 正在向天地一体化方向演进。卫星网络作为空间网络的重要组成部分, 与地面网络相比具有覆盖范围广的优势。为了实现更加灵活的卫星网络组网, 并为地面终端提供不受时、空限制的多样化、高质量信息服务, 软件定义卫星网络技术近年来受到学术界的广泛关注[1-3]。

软件定义卫星网络是软件定义网络技术核心思想与卫星网络的有机融合[4-20], 即: 将控制面功能从中、低轨卫星节点剖离, 并使用地球同步轨道卫星与地面卫星网络管理中心相互协同的控制中、低轨道卫星节点的数据转发。目前国内外学者在软件定义卫星网络架构设计和控制策略优化等方面进行了大量有益的探讨(详见本文 2.1 小节), 但是, 对其安全机制的设计却有待深入的探讨[21]。

众所周知, 接入认证是保障网络安全的重要基础之一。由于卫星网络广域覆盖, 以及中、低轨卫星与地面端用户设备(以下简称“端设备”)间运动非同步性等特点, 大量的端设备不得不主动或被动的与卫星网络较频繁的发生接入认证。但是, 传统卫星网络接入认证机制[21,22]由于以下两方面原因面临着安全性与可用性双重挑战:

1) 传统卫星网络接入认证机制[1-3,23-31]在空间链路开放性方面考虑不足, 对发起接入认证的地面端用户设备的身份合法性缺少判定, 将导致卫星网络面临针对接入认证的拒绝服务攻击的威胁。

2) 由于空间拓扑高动态、星地传输时延方差大, 通过端用户设备频繁与过顶卫星交互的方式进行重接入认证[21-22], 易带来信任关系建立失败、合法端用户设备访问中断等问题。

为了解决以上问题, 本文提出了一种面向软件定义卫星网络的协同接入认证机制, 该机制在充分利用软件定义卫星网络灵活组网技术特点的基础上, 以地面合法端用户设备的身份作为序参量, 并基于序参量实现对接入认证过程的协同控制, 仅对合法端用户设备的接入认证请求和访问进行处理, 可抵抗接入认证的拒绝服务攻击; 同时, 该接入认证机制充分利用地球同步轨道卫星与地面卫星网络管理中心具备稳定管控链路、地球同步轨道卫星具有全局视角的特点, 通过地球同步轨道卫星控制合法端用户设备的切换过程, 保障合法端用户设备访问的连续性。

本文提出的接入认证机制采用基于椭圆曲线无证书算法实现, 控制参数由私钥参与生成, 私钥的安全性由离散对数的难解性保证。

本文中的合法端用户设备定义为通过卫星网络管理中心注册的地面终端, 能够正常获取密钥数据; 攻击者为未通过卫星网络管理中心注册的地面终端, 无法正常获取密钥数据。另外, 考虑到地面合法端用户终端移动化所引入的易失、使用环境不确定等特点, 地面合法端用户设备的私钥由口令加密保存在智能卡中, 攻击者难以获取。

本文主要贡献总结如下:

1) 为了抵御软件定义卫星网络接入认证拒绝服务攻击, 设计了一种协同接入认证模型。该模型充分利用软件定义卫星网络管理面、控制面、转发面的分层结构, 将合法端用户设备的身份标识作为序参量, 建立了软件定义卫星网络多层协同机制。管理面由身份标识生成合法端用户设备同步控制参数, 控制面根据端用户同步控制参数结合身份标识映射为转发控制参数, 转发面根据转发控制参数映射为转发流表, 该模型通过转发流表控制数据面仅上报合法地面注册终端的接入认证请求到控制面, 使控制面对地面攻击者不可见, 减少了软件定义卫星网络所暴露的攻击面, 地面攻击者将难以利用卫星网络链路开放性对接入认证服务发起拒绝服务攻击。

2) 为了解决软件定义卫星网络中空间拓扑高动态、星地传输时延方差大引起的端用户设备切换失败、访问中断的问题, 提出了空间网络拓扑动态变化高容忍的接入认证协议。该协议分为六个阶段, 采用基于椭圆曲线的无证书算法, 将地球同步轨道卫星作为软件定义卫星网络控制面节点, 地球同步轨道卫星具有全局视角、具备一定计算能力, 能够在预接入和接入认证阶段动态更新转发控制参数, 避免地面合法端用户设备通过与多颗卫星交互的方式进行切换, 降低了地面合法端用户设备的重认证次数, 实现了访问的连续性。

3)经过安全性分析, 本文提出的接入认证机制能够在满足传统安全性需求的基础上, 抵御拒绝服务攻击; 经过开销分析, 本文提出的接入认证机制不但能够以不小于 90%的概率将算法执行开销控制在毫秒级, 而且不增加合法端用户设备的重认证次数, 能够提供较好的访问体验。

本文的其余部分组织如下: 第二章对软件定义卫星网络和卫星网络接入认证领域的相关工作进行了总结和分析, 凝练出本文的安全需求; 第三章对面向软件定义卫星网络的多层协同的接入认证模型

及其运行机制进行了详细介绍; 第四章对空间网络拓扑变化高容忍的接入认证协议的六个阶段进行了详尽的描述; 第五章对协议的安全性进行了对比分析; 第六章对协议的开销进行了对比分析; 第七章对本文进行了总结, 并展望了未来的工作。

## 2 相关工作及安全需求

### 2.1 软件定义卫星网络

近些年, 学术界对于软件定义卫星网络架构设计与控制策略优化等方向的研究投入了极大的热情。

Kapovits 等人[4]率先提出通过软件定义网络(Software Defined Networks, SDN)技术的应用, 实现未来服务对卫星网络集成的想法。在文献[4]所提出的想法基础上, Bao 等人[5]设计了一种软件定义卫星网络架构 OpenSAN, 该架构基于解耦卫星网络数据面和控制面以获得高效、细粒度、灵活的组网控制。Tang 等人[6]除提出使用星间链路和地球同步轨道卫星(Geostationary Earth orbit, GEO)广播链路作为控制通道实现网络状态和分发控制消息更新的软件定义卫星网络架构之外, 还进一步分析了软件定义卫星网络的优势和面临的挑战。Barritt 等人[7]进一步细化了如何基于 SDN 技术控制低轨道卫星(Low Earth orbit, LEO)网络的方法, 并提出时空 SDN 技术。

随着网络虚拟化技术(Network Functions Virtualization, NFV)的发展, 开始有学者将网络功能虚拟化技术应用于卫星网络。Gardikis 等人[8]将 NFV 应用在卫星网络中, 并且分析了该技术的优势和挑战; 在此基础上, Gardikis 等人[9]又结合实际应用场景, 分析了将 SDN/NFV 整合在卫星基础设施中的方法, 并提出了基于 SDN/NFV 的层次化架构。

在天地一体化进程的推动下, 学者开始探索 SDN/NFV 技术在天地一体化领域的应用, 主要解决 SDN/NFV 与现有地面网络架构相融合的问题。Agapiou 等人[32]设计的天地一体化架构, 将 NFV 与卫星通信网络相结合, 并使用 SDN 实现天地资源的统一管理。Ferrús 等人在文献[10]中分析了将 SDN/NFV 应用于天地一体化网络中的优势和挑战, 在[11]中阐述了基于 SDN/NFV 技术实现卫星通信与 5G 系统相融合的架构, 并在[12]中提出卫星通信服务动态编排技术。Ahmed 等人在文献[13]与[14]中提出了一种软件定义卫星通信网络与 5G 云基带融合的架构(SatCloudRAN)及其具体部署方法。Huang 等人[15]将 SDN/NFV、边缘计算与天地一体化网络相融合, 实现通信、计算多种资源的统一管理和协同调度。Shuang 等人[20]通过将 NFV 与软件定义无线电相融合设计了一种新的卫星网络架构(SoftSpace)。

除了上述基于 SDN/NFV 设计天地一体化网络架构之外, 在资源管理、路由调度等技术也吸引了大量的研究。例如, Shi 等人[17]提出了基于 OpenFlow 的天地一体化网络架构, 并且设计了从物理资源到应用资源的多种管理策略。Miao 等人[18]基于 SDN 天地一体化网络架构提出了基础应用。Sheng 等人[19]设计了灵活可配置的网络架构, 该架构适用于宽带卫星网络的资源管理, 同时囊括了 SDN/NFV、资源管理架构和资源分配策略。Wang 等人[16]提出基于 SDN/NFV 的卫星网络架构, 该架构能够支持动态负载均衡、路由调度、资源管理等功能。

### 2.2 卫星网络接入认证

接入认证是保障卫星网络安全的基础。但是, 针对卫星网络接入认证机制的研究, 大多数基于简化的卫星网络通信模型; 认证协议设计经历了由基于开销较高的公钥密码算法向基于哈希、异或等开销较小运算构成的算法演进的过程。

Cruickshank 等人[23]提出了一种基于公钥加密(Public Key Cryptography, PKC)的接入认证机制, 该方法支持卫星和端设备间的双向认证, 但是由于基于 PKC 导致其计算复杂较高。Hwang 等人[24]使用地面网关作为管理中心为端用户分配身份信息和密钥, 网络控制中心(Network Control Center, NCC)基于此对接入卫星的端用户进行认证; 由于[24]所提方法基于对称加密算法, 引入了密钥管理和分发的开销, 因此 Hwang 等人在文献[24]中提出了改进方案, 即不再通过地面网关分发密钥, 而是通过网络控制中心基于旧会话密钥保护传递新的会话密钥、临时身份给端用户, 进而在降低密钥分发开销的同时, 可以有效的保护端用户的真实身份。

以上方法采用公钥或者分组密码算法来保障接入认证协议消息的安全, 算法执行开销较高, 而且依赖于旧会话密钥生成新的会话密钥, 前向安全性保证不够。针对这些问题, Chang 等人[25]提出了一种仅采用哈希和异或运算的高效的接入认证机制, 在减少端用户和 NCC 计算量的同时保证了前向安全。该方法虽然降低了算法开销, 但是由于多次接入认证均采用相同的临时身份, 存在端用户访问隐私泄露的问题。Chen 等人[26]提出了一种自认证的方法, 该方法端用户临时身份在每次接入认证时更新, 且由临时身份作为生成会话密钥的参数, 解决端用户访问隐私泄露的问题, 实现 NCC 和端用户双向认证, 但是该方法的验证表存储敏感信息, 有可能导致

NCC 私钥以及端用户主密钥泄露而带来的数据安全问题。为了解决验证表保存敏感数据所带来的数据安全问题, Lee 等人[28]、Yoon 等人[5]和 Tsai 等人[27]通过不存储敏感信息或者不使用验证表的方式, 解决了数据安全问题。

以上方法虽然解决了双向认证、前后向安全、身份隐私安全、数据安全的问题, 但是由于协议中, 端用户和 NCC 之间保存的临时身份不同步, 被证明会被攻击者利用发动重放、拒绝服务等网络攻击, 使端用户无法正常接入网络。为此 Lasc 等人[1]通过 NCC 保留上一次会话临时身份的方法提出了针对该问题的解决思路。但是该解决思路仍然存在重放和身份伪造的问题, 因此, Chang 等人[29]、Zhang 等人[3]、Tsai 等人[31]和 Liu 等人[33]进行了改进, 通过在端用户和 NCC 之间同步临时身份的方法, 确保协议能够抵抗网络攻击。

上述方法由于并未充分考虑空间网络拓扑易变性对接入认证带来的影响, 难以应用于实际环境。为了解决该问题, Yang 等人[34]设计了一种由低轨卫星直接进行接入认证的方法, 该方法利用卫星节点具备一定计算能力的特点, 采用代理认证及群签名技术对端用户进行认证。尽管该方法可减少由于拓扑易变所引入的认证时延, 但是对切换过程处理与实际网络空间环境还有所差异。

根据以上分析, 表 1 选取有代表性的卫星网络接入认证机制, 从安全性和高可用性方面进行了对比。由对比可知, 已有接入认证机制虽然能够满足传统接入认证的安全需求, 但是由于对软件定义卫星网络的空间链路开放性、拓扑高度动态化等特点考虑不足, 接入认证机制难以抵抗拒绝服务攻击, 同时, 在保障地面合法端用户设备访问连续性方面还有所欠缺。

**表 1 典型接入认证方法对比**

**Table 1 Comparison of representative authentication schemes**

| 方法 \ 对比项 | 双向认证 | 隐私保护 | 抗身份伪造 | 网络安全 | | 前/后向安全 | 数据安全 | 抗拒绝服务 | | | 访问连续性 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 抗中间人 | 抗重放攻击 | | | 针对接入认证服务 | 针对合法端用户 | 针对转发节点 | |
| [40] | 否 | 是 | 是 | 是 | 是 | 否 | 否 | 否 | 否 | - | 否 |
| [7] | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 否 | - | 否 |
| [10] | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | - | 否 |
| [36] | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | - | 否 |
| [44] | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | - | 否 |

### 2.3 安全需求

根据 2.2 小节的分析, 本文所要设计的接入认证机制将在满足双向认证、隐私保护、抗身份伪造、网络安全、前向/后向安全、数据安全等基本安全需求的基础上, 重点考虑抗拒绝服务攻击与保证访问连续性的安全需求, 具体而言:

1) 接入认证机制应能够抵抗针对接入认证服务的拒绝服务攻击, 尤其可抵御软件定义卫星网络的控制面饱和攻击;

2) 接入认证机制应能够抵抗由于端用户设备和接入认证服务之间由于身份不同步而引起的针对合法端用户设备的拒绝服务攻击;

3) 接入认证机制应能够抵抗针对转发节点的拒绝服务攻击。(通过耗尽转发面节点带宽、计算资源而非协议安全性漏洞的拒绝服务攻击不在本文的论证范围内)

4) 卫星过顶切换的过程对合法端用户设备无感知, 不会因为过顶卫星之间状态同步失败, 导致合法端用户设备访问中断。

## 3 协同接入认证模型

本章节将介绍软件定义卫星网络协同接入认证模型, 该模型基于图 1 的系统模型提出, 为了不失一般性, 该系统模型可按物理位置划分为地面段、空间段和用户段三部分[20,35-38]。

1) 地面段: 由地面站(Ground Station, GS)、卫星网关(Satellite Gateway, SGW)、地面骨干网和因特网组成, 支持端用户设备通过卫星链路访问地面服务。

2) 空间段: 由 GEO、MEO/LEO 卫星组成, 可提供传统通信、导航和遥感服务; 借助卫星自身计算能力的增强[39], 可支持路由计算、接入认证、安全防护等对计算要求较高的功能。

3) 用户段: 由端用户设备(Satellite Terminal, ST)组成, 端设备可直接接入卫星网络或者通过地面站接入卫星网络, 进而直接访问空间段卫星网络提供的服务, 或者访问地面段提供的服务。

基于上述系统模型, 我们将认证相关的逻辑功能分为管理面、控制面和转发面。

1) 管理面由卫星网络管理中心节点(Sattellite Network Management Centre, SNMC)组成, 支持随网络规模的增加而横向扩展, 该节点部署在地面段网络中, 与空间段高轨卫星保持稳定的通信链路, 具备足够的计算能力, 提供节点管理和安全策略管理功能。

其中, 节点管理为空间网络中的所有节点提供注册、注销、查询等功能, 通过统一标识向量 $ID=\{type,idno,res\}$ 对接点进行管理, *type* 表示节点类型, 如卫星节点、端用户设备、卫星天线、地面站等; *idno* 为节点编码, 为了支持跨域切换, 该编码可区分节点的归属域和身份; *res* 表示节点能够提供或访问的服务类型信息, 例如, 对于卫星节点, *res* 表示能够提供的服务类型, 而对于端用户设备, *res* 则表示能够访问的服务类型。

安全策略管理基于上述命名方式, 从控制面收集各上报数据以判断各节点状态, 并生成安全策略, 实现空间网络节点接入时长、访问服务类型等属性的控制。

除此之外, 管理中心节点承担可信第三方的角色, 负责分发空间网络中控制转发设备的私钥、合法端用户设备的部分私钥及实体间交互所需的控制参数。

2) 控制面由地面段网络控制节点(Network Control Centre, NCC)和空间段 GEO 两部分组成。

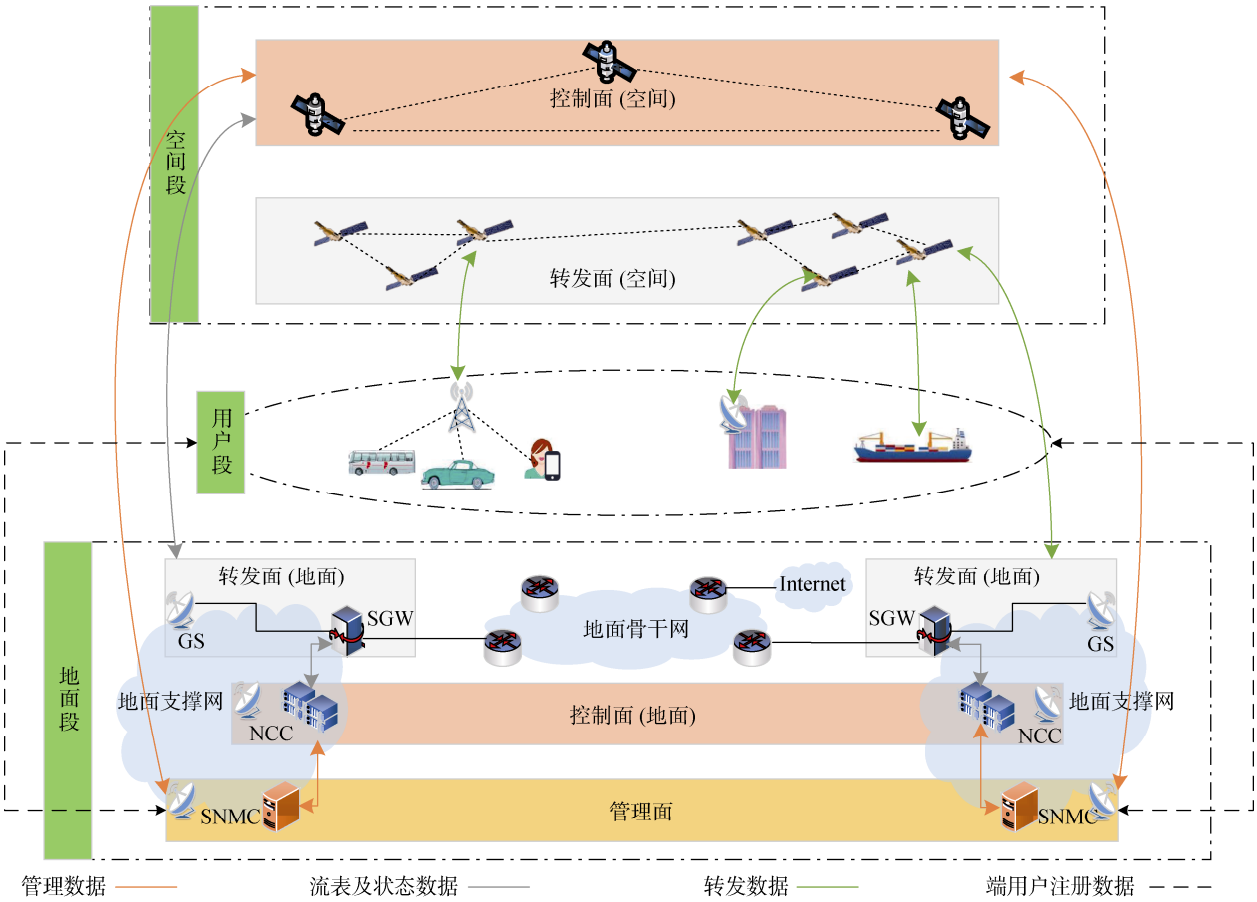


**图 1 系统模型示意图**

**Figure 1 An Illustration of System Model**

网络控制节点部署在地面段的地面支撑网中, 具有足够的计算能力, 该类节点承担地面控制节点的角色。

空间段 GEO 能够获取卫星网络的全局状态, 具备一定计算能力, 并且与 SNMC 及其他地球同步轨道卫星有稳定的通信链路, 该类节点承担空间控制节点的角色, 在本文设计的模型中实现两部分功能:

- 从 SNMC 获取地面合法端用户设备的信息, 基于此, 处理 MEO/LEO 转发的由地面合法端用户设备发起的用户认证请求;
- 通过标准协议接口下发转发面控制信息, 确保仅有合法端用户设备的访问请求能够被转发。

3) 转发面由地面段的 GS、SGW 以空间段节点组成。

GS 和 SGW 部署在地面段的地面支撑网中, 具备足够的计算能力, 该类节点通常结合网络功能虚拟化技术[7,10,11,13,40-42], 执行服务质量保证、防火墙等功能, 在本文设计的模型中, GS 用于接收通过接入认证的合法端用户设备发出的访问请求。

空间段节点具备一定的计算能力, 该类节点能够通过微波通道接收控制面 GEO 发送的数据, 承担空间网络转发节点的角色, 在本文模型中实现两部分功能:

- 接收所连接控制面 GEO 下发的流表信息;
- 对合法端用户设备发起的接入认证请求和访问请求、GEO 返回的接入认证响应进行转发, 对非授权端用户的任何请求不予转发和响应。

基于以上软件定义卫星网络系统模型, 为了实现管理面、控制面、转发面的协同, 本文模型以合法端用户设备的身份标识作为序参量, 并通过序参量为软件定义卫星网络各个层面生成控制参数, 管理面生成同步控制参数($R$), 控制面生成转发控制参数($C$), 转发面生成转发流表($F$), 对接入认证请求、访问请求进行协同控制, 具体流程见图 2, 步骤描述如下:

1) 在管理面, 基于注册合法端用户设备的身份标识, 与控制面节点私钥生成同步控制参数($R$), 管理面通过安全信道将已注册的合法端用户的同步控制参数传递给控制面;

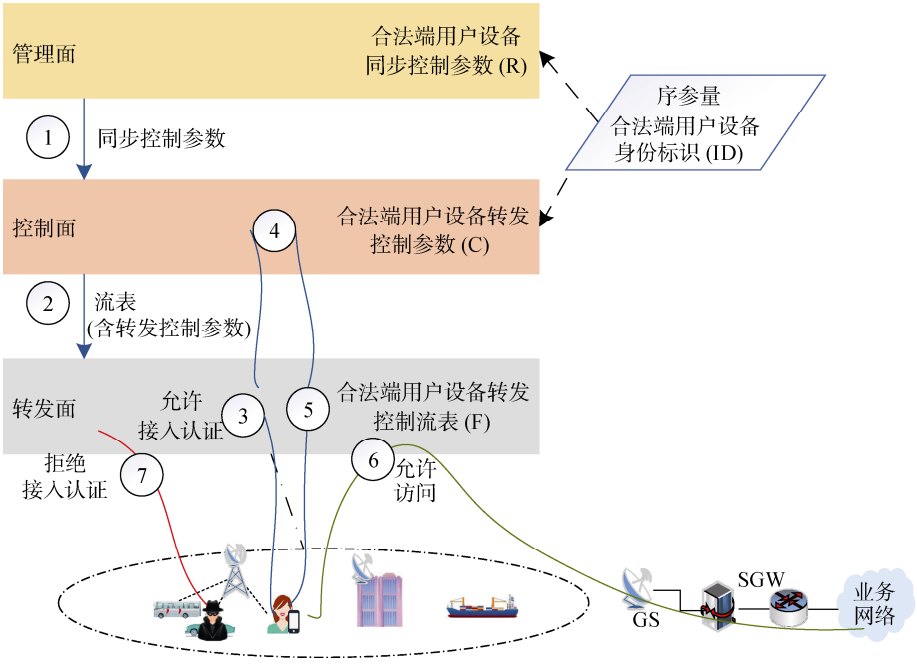


**图 2 基于序参量的协同控制**

**Figure 2 Synergetic control based on order-parameter**

2) 在控制面, 合法端用户设备的身份标识与同步控制参数运算, 生成转发控制参数($C$), 该参数用于控制转发面可接收处理的端用户设备接入认证请求, 控制面通过安全信道将包含转发控制参数的流表传递给转发面;

3) 当已注册合法端用户发起接入认证请求时, 转发面基于流表($F$)判断请求是否来自已注册合法端用户设备, 判断无误后, 将接入认证请求上报至控制面;

4) 控制面验证合法端用户接入认证请求后, 响应端用户接入认证请求, 并通过安全信道将包含新的转发控制参数的流表传递给转发面;

5) 转发面删除用于转发合法端用户接入认证请求的流表, 生效包含新的转发控制参数的流表, 并转发接入认证响应至合法端用户设备, 认证过程结束;

6) 当合法端用户发起访问请求时, 转发面基于新的流表($F$)判断请求是否来自已注册合法端用户设备, 判断无误后, 将访问请求转发至对应的地面站进行处理;

7) 当攻击者发起攻击时, 由于攻击者访问难以携带正确的转发控制参数, 因此, 转发面基于流表($F$)将拒绝攻击者的一切访问, 包括接入认证请求和访问请求。

与传统卫星网络通信模型相比, 本文提出的软件定义卫星网络接入认证模型基于序参量实现软件定义卫星网络各层面的协同, 能够抵抗针对接入认证服务的拒绝服务攻击。与[28,29,34,43]中直接转发

接入认证请求的方法不同, 通过转发控制参数, 空间段 GEO 可对 MEO/LEO 进行控制, 确保仅有合法端用户的接入认证请求能够发至空间段 GEO 中, 极大的减少了软件定义卫星网络所暴露的攻击面, 攻击者将难以利用卫星网络链路开放性发起接入认证拒绝服务攻击。

## 4 空间拓扑动态变化高容忍的接入认证协议

本章节将介绍抗空间拓扑高动态变化的接入认证协议, 该协议充分利用空间段地面同步轨道卫星控制节点具有全局视角、具备一定计算能力的特点, 由地球同步轨道卫星主动更新转发控制参数, 确保仅地面合法端用户设备能够访问接入认证服务, 同时, 地面合法端用户设备在卫星过顶切换过程中无须在多星间同步信息, 保障合法端用户设备访问的连续性, 满足可用性需求。

为了方便描述, 对协议参与方所使用的符号定义如下:

**表 2 协议参与方对应表**

**Table 2 Table of protocol participant notations**

| 协议参与方符号 | 解释 |
|---|---|
| SNMC | 卫星网络管理中心 |
| CGEO | 空间段地面同步轨道卫星控制节点 |
| GS | 地面站 |
| FLEO | 转发面低轨卫星 |
| ST | 端用户设备(简称: 端用户) |

### 4.1 安全假设

本文所设计的接入认证协议具有如下安全假设:

1) 模型中所有实体均使用统一初始参数;

2) SNMC 作为可信的密钥分发中心, 在生成域参数的同时, 参与实体部分公私钥的生成过程, 并能够以安全的方式传递给参与该协议的所有实体;

3) SNMC 与 CGEO 之间, CGEO 与 GS 之间, CGEO 与 LEO 之间以及 CGEO 之间均能够建立安全的通信链路;

4) 外部节点是潜在的恶意攻击者, 其中外部攻击者的攻击目标是对软件定义卫星网络进行破坏, 或者伪造成合法端用户接入并访问软件定义卫星网络。检测识别内部节点由正常用户演变为恶意用户, 进而发起攻击不属于本文的研究范畴。

### 4.2 协议设计

本文设计的接入认证协议由初始化阶段、转发控制节点注册阶段、端用户注册阶段、预接入阶段、端用户接入认证阶段、数据转发阶段六个阶段组成, 主要流程如图 3 所示。

协议基于椭圆曲线无证书算法设计, 在预接入阶段, 当合法 ST 注册成功后, 由 SNMC 生成同步控制参数, 并向 CGEO 分发注册的 ST 信息, CGEO 将根据该参数进一步生成包含转发控制参数的流表, 下发给 FLEO, FLEO 基于流表控制仅有合法端用户的接入认证请求才能够上报给 CGEO 进行处理; 当合法 ST 的会话到期或者 CGEO 覆盖范围内的 FLEO 位置发生变化时, 由 CGEO 根据当前已接入合法 ST 的状态及 FLEO 的位置更新转发控制参数, 并以流表方式下发给 FLEO, 若合法 ST 会话到期, FLEO 将转发接入认证请求至 CGEO, 若合法 ST 会话未到期, FLEO 将继续转发 ST 访问请求到 GS。

在端用户接入认证阶段, 合法 ST 完成接入认证过程, 由 CGEO 更新转发控制参数并以流表方式下发给 FLEO, FLEO 基于流表控制将合法 ST 访问请求转发至 GS, 外部攻击者重放的接入认证请求将由于转发控制参数不匹配被 FLEO 丢弃。

通过以上步骤, CGEO 仅在接入认证时, 对合法端用户设备可见, 减少 CGEO 暴露的攻击面; 同时, CGEO 具备全局视角, 能够根据 FLEO 的空间位置以及合法 ST 的接入状态更新转发控制参数, 保障合法 ST 访问的连续性。

#### 4.2.1 初始化阶段

在初始化阶段, SNMC 作为部分密钥管理中心, 选择椭圆曲线, 完成空间节点安全参数的生成。详细步骤如下:

1) SNMC 选择一个 $K$ 位长的素数 $p$, 生成椭圆曲线参数有限域 $F_p$、定义在该有限域上的椭圆曲线 $E(F_p)$, 选择 $P \in E(F_p)$, 阶为 $q$;

2) 随机选择 $s \in Z_q^*$, 基于此计算 $P_{pub} = s \cdot P$;

3) SNMC 选择满足 $\{0,1\}^* \to Z_q^*$ 的哈希函数 $H_1$, 选择满足 $Z_q^* \to \{0,1\}^n$ 的哈希函数 $H_2$;

4) SNMC 秘密保存 $s$, 并公开安全参数 $params = \langle F_p, E(F_p), P, P_{pub}, H_1, H_2 \rangle$。

#### 4.2.2 转发控制节点注册阶段

SNMC 为除 ST 之外实体提供的注册过程称为转发控制节点注册, 包括 FLEO、CGEO 和 GS 等。以上节点在其发射或者部署之前, 均可以采用离线方式从 SNMC 中获取注册信息, 以保证注册过程的安全性, 具体过程见算法 1。

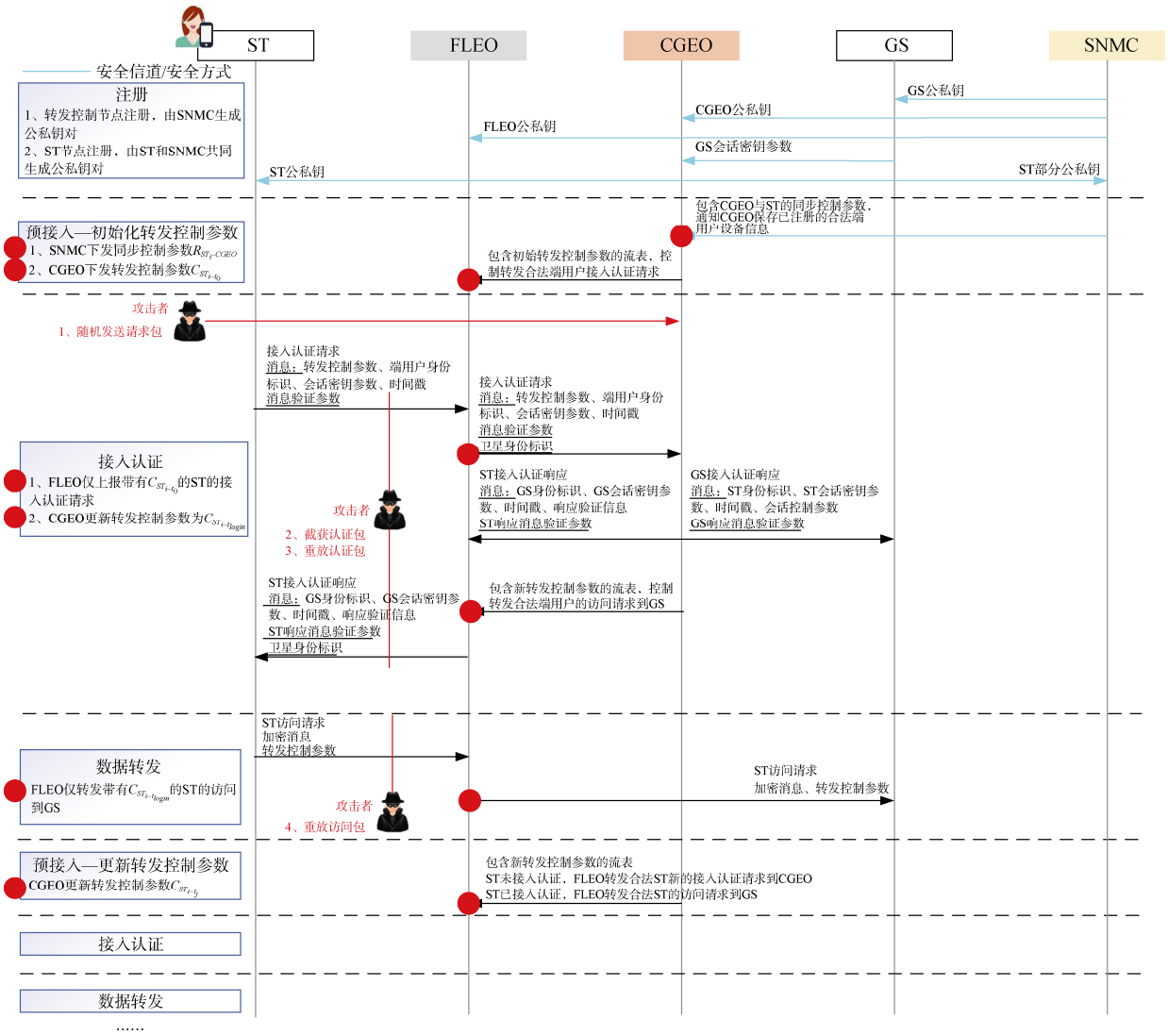


**图 3　合法端用户接入与访问流程以及攻击者攻击方法**

**Figure 3　Legitimate STs access and request process, and attackers attack schema**

**算法 1.转发控制节点注册.**

输入: 转发控制节点序列号 *EID*

输出: SNMC 输出转发控制节点参数 $M_E$

**过程 1: 转发控制节点生成序列号**

1) 转发控制节点基于硬件信息生成 *EID*;

2) 转发控制节点将 *EID* 作为输入参数传递给 *SNMC*;

**过程 2: SNMC 生成转发控制节点参数**

1) 根据空间节点命名规则设置 $ID_E=\langle type, EID, res\rangle$;

2) 选择随机数 $s_E\in Z_q^*$, 计算 $D_E=s_E\cdot P$;

3) 设置 $\varepsilon_E=s\cdot H_1\left(D_E, ID_E\right)+s_E$;

4) 将 $M_E=\langle params, \varepsilon_E, D_E, ID_E, ID_{GS}\rangle$ 以安全的方式发送给转发控制节点。

**过程 3: 转发控制节点校验存储参数**

1) 转发控制节点接收 $M_E$;

2) 计算 $\varepsilon_E\cdot P=P_{pub}\cdot H_1\left(D_E, ID_E\right)+D_E$ 是否成立, 如果成立, 接收并秘密存储 $\varepsilon_E$ 作为私钥, 否则拒绝参数。

**过程 4: GS 向 CGEO 传递会话密钥参数**

1) GS 选择随机数 $\mu_{GS}, \gamma_{GS}\in Z_q^*$, 计算得到 $g_{GS}=\mu_{GS}\cdot P$;

2) GS 采用安全信道与 CGEO 传递参数 $\langle ID_{GS}, g_{GS}, \gamma_{GS}\rangle$。

### 4.2.3　端用户注册阶段

端用户注册阶段, 经过端用户注册阶段的地面终端称为合法端用户设备。

合法 ST 和 SNMC 将基于椭圆曲线无证书算法共同生成公私钥对(算法 2 中过程 1 和过程 2), 私钥以安全的方式通过口令加密保存在合法ST的智能卡中(算法 2 中过程 3), 同时 SNMC 将合法端用户设备的公开信息保存在注册表中(算法 2 中过程 4)。

为了保障注册过程的安全, 合法ST与SNMC之间通信应采用如 TLS 等地面网络常用的安全协议, 由于本文主要关注接入认证过程, 地面网络通信的安全保障技术不在此详细讨论, 同时, 注册采用基于椭圆曲线无证书算法。

**算法 2.端用户注册.**

输入: ST 身份标识 $UID$

输出: SNMC 输出端用户参数 $M_{ST}$, ST 输出 $PK_{ST}$

**过程 1: ST 设定端用户密钥**

1) 自行选择身份标识 $UID$;

2) 选择 $x_{ST} \in Z_q^*$ 作为部分私钥;

3) 计算 $X_{ST} = x_{ST} \cdot P$ 作为部分公钥;

4) 设置 $TID = H_2\left(UID, x_{ST}\right)$;

**过程 2: SNMC 提取部分密钥**

1) 根据空间节点命名规则设置 $ID_{ST} = \langle type, TID, res \rangle$, 并依据此计算 $r_{ST} = H_2\left(ID_{ST}, s\right)$;

2) 将 $CGEO$ 和 $GS$ 的信息进行组装记为 $I_{CGEO} = \langle ID_{CGEO}, O_{CGEO}, ID_{GS} \rangle$, 其中 $O_{CGEO}$ 为 $CGEO$ 的信息;

3) 随机选择 $s_{ST} \in Z_q^*$, 计算 $D_{ST} = s_{ST} \cdot P$, 其中将 $D_{ST}$ 作为该 $ST$ 的部分公钥;

4) 计算 $\varepsilon_{ST} = s_{ST} + s \cdot H_1(ID_{ST}, D_{ST}, X_{ST}, r_{ST})$, 作为端用户 $ST$ 的部分私钥;

5) 计算 $M_{ST} = \langle params, \varepsilon_{ST}, ID_{ST}, D_{ST}, I_{CGEO}, r_{ST} \rangle$, 并通过安全的方式传递给 $ST$。

**过程 3: ST 验证 SNMC 输出参数**

1) 接受并进行如下等式的判断, 如果成立则接收提取部分私钥, 否则拒绝接受部分私钥 $\varepsilon_{ST} \cdot P = D_{ST} + P_{pub} \cdot H_1(ID_{ST}, D_{ST}, X_{ST}, r_{ST})$;

2) 设置私钥为 $S_{ST} = (x_{ST}, \varepsilon_{ST})$

3) 设置公钥为 $PK_{ST} = (X_{ST}, D_{ST})$

4) 将私钥以及 $r_{ST}$ 一起保存在智能卡中, 并只能够由口令解密执行计算;

5) 将 $PK_{ST}$ 发送给 SNMC。

**过程 4: SNMC 保存参数**

1)在验证表中保存 $\langle PK_{ST}, ID_{ST} \rangle$.

#### 4.2.4 预接入阶段

在该阶段, CGEO基于SNMC发送的信息更新转发面消息转发控制参数, 确保只有已注册合法 ST 能够执行接入认证过程。该过程分为两种情况:

一种是ST注册通过之后, 由SNMC触发执行预接入过程(算法 3), 该过程由 SNMC 将注册的合法端用户设备信息转换为同步控制参数, 并通过安全信道传递给CGEO(算法 3 过程 1); CGEO根据同步控制参数生成转发控制参数, 并以流表方式下发给FLEO(算法 3 过程 2), 确保仅有注册的合法端用户设备发起的接入认证请求能够上报给 CGEO。

一种是合法 ST 会话时间到期之后, 由 CGEO 触发执行预接入过程。该过程由 CGEO 触发, 发生在合法端用户会话信息失效或者安全状态改变时, CGEO 通过更新 FLEO 的转发控制参数, 控制 ST 重新发起接入认证请求。

**算法 3.由 SNMC 触发的预接入.**

输入: 为 ST 选取的随机数 $r_{ST_i}$

输出: 消息转发控制参数 $C_{ST_i}$

**过程 1: SNMC 生成通信参数**

1) 设置端用户和控制面高轨卫星的同步控制参数 $R_{ST_i-CGEO} = \varepsilon_{CGEO} \oplus r_{ST_i}$;

2) 设置控制面高轨卫星与端用户的通信参数 $M_{ST_i-CGEO} = \left\langle PK_{ST_i}, ID_{ST_i}, R_{ST_i-CGEO} \right\rangle$;

3) 将 $M_{ST_i-CGEO}$ 通过安全信道传输给 CGEO。

**过程 2: CGEO 生成消息转发控制参数**

1) CGEO 接收 $M_{ST_i-CGEO}$;

2) 提取端用户 $ID_{ST_i}$, 使用私钥提取控制面高轨卫星与端用户的同步控制参数 $R_{ST_i-CGEO}$, 计算 $r_{ST_i} = \varepsilon_{CGEO} \oplus R_{ST_i-CGEO}$;

3) 设置控制面高轨卫星对该端用户的消息转发控制参数初始值 $C_{ST_i} = H_2\left(ID_{ST_i}, r_{ST_i} + 1\right)$;

4) 更新 $M_{ST_i-CGEO}$;

5) 在验证表 $VerTable$ 中新增验证表项, 记为 $V_i = \left\langle M_{ST_i-CGEO}, state_i, se_i \right\rangle$, 其中 $1 \leqslant i \leqslant N$, $N$ 是端用户的数量, $state$ 是端用户当前的状态信息, 包括未认证和已认证两种; $se$ 是端用户的安全控制信息, 包括网络接入时间 $t_{login}$、空间网络可使用时长 $t_{last}$。并使用安全信道与其他 CGEO 进行信息同步, 验证表为端用户验证表项的集合。

6) 采用南向接口向其覆盖范围内的 FLEO 下发

转发面控制流表, 单条流表包含流表匹配域和执行动作, 其中流表匹配域为消息转发控制参数 $C_{ST_i}$, 执行动作为上报消息, 当端用户携带消息转发控制参数发起认证时, FLEO 将上报认证请求。

**算法 4.由 CGEO 触发的预接入.**

输入: 验证表 *VerTable*

输出: 消息转发控制参数 $C_{ST_i}$

**过程 1: CGEO 生成消息转发控制参数**

1) 提取验证表中的 *se*, 判断 $t_{cur} \geqslant t_{login} + t_{last}$ 是否成立, 如果成立则证明端用户的会话已经失效, FLEO 中的转发流表已经过期, 继续执行如下步骤;

2) 提取 $ID_{ST_i}$, 并计算 $r_{ST_i}$;

3) 更新控制面高轨卫星对该端用户的消息转发控制参数 $C_{ST_i} = H_2\left(ID_{ST_i}, r_{ST_i} + ran\left(t_{login}\right)+1\right)$;

4) 更新 $V_i$, 包括更新 $M_{ST_i-CGEO}$, 设置验证表中会话失效的端用户的 *state* 项为未认证, 同时重置 *se* 中的 $t_{login}$, 使用安全信道与其他 CGEO 进行信息同步;

5) 采用南向接口向其覆盖范围内的 FLEO 下发更新后的转发面控制流表, 单条流表包含流表匹配域和执行动作, 当端用户携带新的消息转发控制参数发起认证时, FLEO 将上报认证请求。

### 4.2.5 接入认证阶段

在该阶段, ST 发起接入认证请求(算法 5), 接入认证请求包含转发控制参数、端用户设备身份、会话密钥参数、时间戳, 以及请求的验证信息, 其中, 转发控制参数只有合法 ST 才能够生成, 时间戳用于抵抗重放攻击。

ST 请求发送到 FLEO, FLEO 对接入认证请求进行处理(算法 6), FLEO 判断数据包是否重放, 并提取请求中的转发控制参数, 判断与预接入阶段设置的是否相匹配, 如果匹配则将接入认证请求转发至 CGEO 进行认证, 如果不匹配将数据包丢弃。

CGEO 执行接入认证(算法 7), 通过无证书算法验证接入认证请求的真实性和完整性, 验证通过后, 更新消息转发控制参数, 确保只有 ST 的访问请求能够通过转发面进行转发, 重放的接入认证请将直接被丢弃, 同时分别向 ST 和 GS 发送响应数据, 实现 ST 和 GS 会话密钥参数的交换。

ST 和 GS 处理响应数据, 并计算得到会话密钥(算法 8 和算法 9), ST 和 GS 接收到响应数据之后, 首先执行对 CGEO 的身份认证, 认证通过后, 更新消息转发控制参数, ST 可以使用更新后的转发控制参数通过 FLEO 访问 GS, GS 根据 CGEO 下发的转发控制参数判断是否将来自 ST 的请求转发至地面网络中对应的服务。

**算法 5. ST 发起接入认证**

输入: $ID_{ST_i}$、ST 私钥、$r_{ST_i}$

输出: 接入认证请求 $M_{R_{ST_i}-CGEO}$、$\sigma_{ST_i}$

1) 设置用户接入认证所需要的消息转发控制参数 $C_{ST_i} = H_2\left(ID_{ST_i}, r_{ST_i} + t_{login-last} + 1\right)$, 首次访问时设置 $t_{login-last} = 0$ ;

2) 选择随机数 $\mu_{ST_i} \in Z_q^*$, 计算 $g_{ST_i} = \mu_{ST_i} \cdot P$;

3) 获取当前时间作为认证时间 $t_{login}$, 设置 $ST_i$ 认证消息 $M_{R_{ST_i}-CGEO} = \left\langle C_{ST_i}, ID_{ST_i}, g_{ST_i}, t_{login} \right\rangle$;

4) 随机选取 $\alpha_{ST_i} \in Z_q^*$, 计算 $Y_{ST_i} = \alpha_{ST_i} \cdot P$;

5) 设置 $h = H_2\left(M_{R_{ST_i}-CGEO}, Y_{ST_i}, PK_{ST}\right)$ ;

6) 设置 $U_{ST_i} = \left(\alpha_{ST_i} + h\right)^{-1}\left(x_{ST} + \varepsilon_{ST}\right)$;

7) 设置 $\sigma_{ST_i} = \left\langle U_{ST_i}, Y_{ST_i} \right\rangle$;

8) 返回 $M_{R_{ST_i}-CGEO} \| \sigma_{ST_i}$ 给 FLEO。

**算法 6. FLEO 处理接入认证请求**

输入: $C_{ST_i}$

输出: 处理结果

1) **IF** 根据控制面下发的流表 $F$ 匹配 $C_{ST_i}$ **AND** 提取时间戳判断数据包是否重放

2) **THEN** 按照流表, 附加 FLEO 标识封装数据包, 将认证时间 $t_{login}$ 记录在流表元数据中, 通过控制通道发送给控制器进行处理

3) **ELSE**

4) 丢弃数据包, 不做任何响应

5) **END IF**

**算法 7. CGEO 处理接入认证请求**

输入: $ID_{ST_i}$ 以及 $M_{R_{ST_i}-CGEO} \| \sigma_{ST_i}$

输出: $S_{ST_i}$ 和 GS 的认证响应 $M_{CGEO-R_{ST_i}} \| \sigma_{CGEO-R_{ST_i}}$ 和 $M_{CGEO-GS} \| \sigma_{CGEO-GS}$

1) 根据 $ID_{ST_i}$ 查找验证表, 提取 $R_{ST_i-CGEO}$, 计算 $r_{ST_i} = \varepsilon_{CGEO} \oplus R_{ST_i-CGEO}$;

2) 计算 $h_\varepsilon = H_1(ID_{ST}, D_{ST}, X_{ST}, r_{ST})$;

3) 计算 $h' = H_2\left(M_{R_{ST_i}-CGEO}, Y_{ST_i}, PK_{ST}\right)$;

4) **IF** $U_{ST_i}\left(Y_{ST_i} + h' \cdot P\right) = X_{ST_i} + D_{ST_i} + P_{pub} \cdot h_\varepsilon$ 不成立

5) **THEN** 丢弃数据包不做响应

6) **ELSE**

7) 接受 $M_{R_{ST_i}-CGEO} \| \sigma_{ST_i}$

8) 设置 $C_{ST_{i-t_{login}}} = H_2\left(ID_{ST_i}, r_{ST_i} + t_{login}\right)$;

9) 随机选取 $\beta \in Z_q^*$, 计算 $L_{CGEO} = \beta \cdot P$;

10) 设置与 $ST_i$ 响应消息为 $M_{CGEO-R_{ST_i}} \| \sigma_{CGEO-R_{ST_i}}$, 其中:

$$M_{CGEO-R_{ST_i}} = \left(ID_{GS}, g_{GS}, t_j, L_{CGEO}\right)$$

$$\sigma_{CGEO-R_{ST_i}} = \varepsilon_{CGEO} \cdot H_2(M_{CGEO-R_{ST_i}}, r_{ST_i}) + \beta$$

11) 设置与 GS 响应消息为 $M_{CGEO-GS} \| \sigma_{CGEO-GS}$, 其中:

$$M_{CGEO-GS} = \left(ID_{ST_i}, C_{ST_{i-t_{login}}}, g_{ST_i}, t_j\right)$$

$$\sigma_{CGEO-GS} = \varepsilon_{CGEO} \cdot H_2(M_{CGEO-GS}, \gamma_{GS}) + \beta$$

12) *CGEO* 将消息同时发送给 $S_{ST_i}$ 和 GS, 并对验证表中的参数 $V_i$ 进行更新, 包括更新 *state* 状态为已接入, 并更新 *sec* 中 $ST_i$ 的认证时间为 $t_{login}$;

13) CGEO 采用南向接口向其覆盖范围内的 FLEO 更新转发面控制流表, 为了确保流表中的转发控制参数不被攻击者利用发起攻击, CGEO 将根合法端用户的登录时间 $t_{login}$, 对转发控制参数设置 *MatchFeild* 的偏移量信息。FLEO 接收到流表更新消息之后, 删除已有流表 $flow_{ST_i}$, 增加流表 $flow_{ST_{i-t_{login}}}$, 并设置该流表的有效时间为 $t_{last}$。

14) 当 $ST_i$ 携带新 $C_{ST_{i-t_{login}}}$ 的消息转发控制参数发起请求时, FLEO 将转发该访问请求到对应的 GS, 当超过有效时间限制之后, 端用户的会话自动结束, 只有 CGEO 重新更新消息转发控制参数之后, $ST_i$ 能够再次接入空间网络。

15) **END IF**

**算法 8. ST 处理认证响应.**

输入: $M_{CGEO-R_{ST_i}} \| \sigma_{CGEO-R_{ST_i}}$

输出: 无

1) 提取 $t_j$ 确保数据未被重放;

2) 计算 $L_1 = P_{pub} \cdot H_1\left(D_{CGEO}, ID_{CGEO}\right) + D_{CGEO}$;

3) 计算 $L_2 = H_2(M_{CGEO-R_{ST_i}}, r_{ST_i})$;

4) **IF** $\sigma_{CGEO-R_{ST_i}} \cdot P - L_{CGEO} = L_1 \cdot L_2$ 不成立

5) **THEN** 拒绝接受该数据

6) **ELSE**

7) 提取 $g_{GS}$, 计算 $sk_{GS-ST_{i-t_j}} = \mu_{ST_i} \cdot g_{GS}$;

8) 设置与 GS 在时间 $t_j$ 的会话密钥为 $sk_{GS-ST_{i-t_j}}$, 会话控制信息为 $C_{ST_{i-t_{login}}}$, 更新 $t_{login\text{-}last} = t_{login}$。

9) **END IF**

**算法 9. GS 处理认证响应.**

输入: $M_{CGEO-GS} \| \sigma_{CGEO-GS}$

输出: 无

1) 提取 $t_j$ 确保数据未被重放;

2) 计算 $L_1 = P_{pub} \cdot H_1\left(D_{CGEO}, ID_{CGEO}\right) + D_{CGEO}$;

3) 计算 $L_2 = H_2(M_{CGEO-GS}, \gamma_{GS})$;

4) **IF** $\sigma_{CGEO-R_{ST_i}} \cdot P - L_{CGEO} = L_1 \cdot L_2$ 不成立

5) **THEN** 拒绝接受该数据

6) **ELSE**

7) 提取 $g_{ST_i}$, 计算 $sk_{GS-ST_{i-t_j}} = \mu_{GS} \cdot g_{ST_i}$;

8) 设置与 $ST_i$ 在时间 $t_j$ 的会话密钥为 $sk_{GS-ST_{i-t_j}}$, 会话控制信息为 $C_{ST_{i-t_{login}}}$。

9) **END IF**

### 4.2.6 数据转发阶段

数据转发阶段, ST 通过接入认证之后将发起访问请求, FLEO 通过 CGEO 下发的新的消息转发控制参数对来自 ST 的访问请求进行转发, 当消息转发控制参数匹配 CGEO 所下发的参数时, 访问请求被转发给 GS, 当消息转发控制参数不匹配 CGEO 所下发的参数时, 访问请求被丢弃。

1) $ST_i$ 发送消息 $m$, 计算 $m_{enc} = Enc_{sk_{GS-ST_{i-t_j}}}(m)$, 组装发送 $M = \left(C_{ST_{i-t_j}}, m_{enc}\right)$, 其中转发控制参数将根据接入认证时间 $t_{login}$ 按照偏移量写入消息 $M$ 的指定位置;

2) FLEO 收到该消息之后, 根据转发面流表判断携带消息转发控制参数的数据是否能够进行转发, 如果流表生效, 则将该消息转发给 GS, 如果的流表已失效, 则不响应数据, 超时后 $ST_i$ 将重新发起接入

认证请求。

## 5 安全性分析

### 5.1 双向认证

在本文提出的协议中, CGEO 通过验证 $U_{ST_i}\left(Y_{ST_i}+h'\cdot P\right)=X_{ST_i}+D_{ST_i}+P_{pub}\cdot h_{\varepsilon}$ 能够唯一确认认证请求来源于 $ST_i$, 因为只有经过注册的合法 $ST_i$ 才能够生成 $U_{ST_i}$。与此同时, $ST_i$ 能够通过 $\sigma_{CGEO-R_{ST_i}}$ 消息验证响应消息来源为 CGEO, 因为该消息只有私钥为 $\varepsilon_{CGEO}$ 的 CGEO 能够生成。综上, $ST_i$ 和 CGEO 之间能够完成双向认证。

### 5.2 身份、位置及访问的隐私保护

在本文提出的协议中, 端用户设备的真实身份信息 $ID_{ST}$ 只有 SNMC、CGEO 可知, FLEO 以及 GS 无法获取真实的端用户信息; 由于 ST 在多个 FLEO 之间切换, 真实的 ST 身份信息无法在同一 FLEO 中进行追踪; GS 虽然能够连续处理同一端用户的请求, 但是处理的消息转发控制参数不断变化, 将无法判断请求是否由同一 ST 发出, 不能追踪 ST 的访问信息。综上, ST 的身份、位置和访问信息是受到保护的。

### 5.3 抗身份伪造攻击

在本文提出的协议中, 通过无证书签名方案, SNMC 仅生成部分私钥, 其余私钥由 ST 自行生成, 外部攻击者难以通过攻击 SNMC 获取是要的方式伪装成合法端用户设备, 发起接入认证请求; 同时, 由于 CGEO 和 FLEO 之间已建立安全控制通道, 外部攻击者难以攻击控制通道, 伪装成 CGEO 攻击端用户。综上, 该协议能够抵抗身份伪造攻击。

### 5.4 抗中间人攻击

在本文提出的协议中, 会话密钥破解的难度依赖于椭圆曲线离散对数问题, 因此 FLEO、攻击者即使获取了 $g_{GS}$ 和 $g_{ST_i}$, 也不能计算得到会话密钥, 进而无法发起中间人攻击。综上, 该协议能够抵抗中间人攻击。

### 5.5 抗重放攻击

在本文提出的协议中, ST 的认证通过之后, FLEO 的会话控制信息将被改变, 攻击者即使获取了认证请求包, 该请求包也将不会被转发至 CGEO; 由 CGEO 发送给 ST 和 GS 的响应消息携带了时间戳信息, 重放的消息将不会被 ST 和 GS 接受。综上, 该协议能够抵抗重放攻击。

### 5.6 前向/后向安全

在本文提出的协议中, ST 和 GS 之间的会话密钥随着会话的不同而不同, 会话密钥之间无联系。综上, 该协议能够满足前向/后向安全的要求。

### 5.7 数据安全

在本文提出的协议中, SNMC 的验证表中存储的内容包括: ST 的公钥; CGEO 的验证表中存储的内容为 ST 的公钥和临时身份信息, 并未存储敏感的信息, 即使盗取也不能获取密钥信息。综上, 该协议能够保证敏感数据的安全。

### 5.8 抗拒绝服务

在本文提出的协议中, 由外部攻击者发起的针对接入认证服务和合法端用户设备的拒绝服务将不容易发生, 攻击方式如图 3 所示。

1) 攻击者通过截获接入认证请求, 并基于此随机构造数据包, 发起软件定义网络的控制面饱和攻击及盲 DDoS 攻击[44]。由于 FLEO 流表中 *MatchFiled* 的值将由 CGEO 控制进行更新, 即接入认证和数据转发将采用不同的消息转发控制参数, 接入认证通后将立即更换消息转发控制参数, 攻击者在接入认证阶段, 即使通过截获合法端用户发送的接入认证请求, 得到转发控制参数, 认证请求也只能被 CGEO 处理一次, 攻击者再次重放该接入认证请求, 由于消息转发控制参数已经更新, 攻击者没有合法端用户的 $r_{ST_i}$ 和 $\mu_{ST_i}$, 无法伪造生成数据转发阶段的消息 $M$, 因此, 攻击者所发送的大量证请求将不会被 FLEO 转发至 CGEO, 不会对 CGEO 产生影响。

2) 攻击者截获并丢弃合法端用户设备的接入认证请求或响应, 针对合法端用户发起拒绝服务攻击, 攻击位置如图 3 所示, 虽然合法端用户的接入认证请求或响应包被截获丢弃, 但是在预接入过程中, CGEO 已经在 FLEO 中设置了消息转发控制参数, 攻击者难以修改, 终端接入认证请求超时之后, 合法端用户能够重新发起被 FLEO 正确转发的接入认证请求, 不受攻击者截获接入认证数据包的影响。

3) 攻击者重放接入认证请求, 针对合法端用户发起拒绝服务攻击, 攻击位置如图 3 所示。攻击者截获合法端用户发来的接入认证请求, 并重放将该请求发送至 FLEO, 由于完成终端接入认证之后, CGEO 立刻在 FLEO 中更新转发控制参数为 $C_{ST_{i-t_{login}}}$, 重放的接入认证请求由于仍携带原有的转发控制参数 $C_{ST_{i-t_0}}$, 将被 FLEO 丢弃。

4)攻击者监听合法端用户访问请求, 获取当前会话的消息转发控制参数, 并伪造数数据包向 FLEO 发起拒绝服务攻击。该请求被 FLEO 转发的条件是, 攻击者能够在会话时长内解析出当前会话的转发控

制参数, 该会话的消息转发控制参数由 CGEO 在接入认证之后更新, 同时根据 ST 的接入认证时间对消息转发控制参数匹配的偏移量在流表中进行了设置, 如果攻击者无法在一个会话时间内正确提取消息转发控制参数, 则将难以伪造合法端用户的访问请求, 发起拒绝服务攻击。

综上, 本文提出的协议能够抵抗针对接入认证服务和合法端用户设备的拒绝服务攻击。

### 5.9 访问连续性

合法端用户设备在完成接入认证的前提下, 当卫星过顶切换时, 将由 CGEO 完成合法端用户设备当前会话中转发控制参数的同步过程, 即将该参数同步到接力服务的 FLEO 中, 由于 FLEO 在 CGEO 的覆盖范围内, 因此, 过顶卫星之间状态同步可靠性较高, 能够保障合法端用户设备访问的连续性。

## 6 开销分析

开销分析对比了本文提出的协议与已有学者提出协议的运行效能, 分为认证时延、重认证时延和认证算法计算时间开销三部分。

### 6.1 认证时延

认证时延由计算时延和交互时延构成, 如下:

1) 计算时延定义为端用户发起认证请求到认证结束所耗费的计算开销, 该指标用于评估认证协议对卫星计算资源的消耗情况。为了能够对计算开销进行准确评估, 本文将认证过程的计算单元划分为哈希运算 $T_h$, 乘法运算 $T_{mul}$, 加法运算 $T_{add}$, 异或运算 $T_{xor}$, 根据文献[34, 43]中的分析, 由于异或运算及哈希运算所产生的开销可忽略, 因此仅估算乘法运算和加法运算所带来的计算时延, 根据文献[45-46], $T_{mul}$ 为 2.21 毫秒, $T_{add}$ 约为 $0.12T_{mul}$, 约为 0.27 毫秒, 计算时延结果对比见表 3。

**表 3 计算时延对比**

**Table 3 Table of computation delay comparison**

| 方法 | 计算时延 | 时延估算(秒) |
|---|---|---|
| Cheng's [29] | $9T_h+5T_{xor}$ | 0 |
| Liu's [43] | $9T_h+5T_{xor}$ | 0 |
| Lee's [28] | $10T_h+7T_{xor}$ | 0 |
| Meng's [34] | $7T_h+10T_{mul}+4T_{add}$ | 0.0231 |
| 本文方法 | $8T_h+10T_{mul}+8T_{add}+T_{xor}$ | 0.0242 |

2) 交互时延定义为空间组件之间在端用户发起接入认证请求到认证结束期间内交互所耗费的时间, 该指标影响端用户接入卫星网络的使用体验。本文将交互时延划分为确定性交互时延和非确定性交互时延, 交互时延的对比结果见表 4。具体而言:

**表 4 交互时延对比**

**Table 4 Table of interaction delay comparison**

| 方法 | 交互时延 | 时间估算(秒)($m$=1) |
|---|---|---|
| Cheng's [29] | $2T_{ST-FL}+m\cdot T_{forward}+T_{compute}+2T_{FL-SN}$ | 2.072 |
| Liu's [43] | $2T_{ST-FL}+m\cdot T_{forward}+T_{compute}+2T_{FL-SN}$ | 2.072 |
| Lee's [28] | $2T_{ST-FL}+m\cdot T_{forward}+T_{compute}+2T_{FL-SN}$ | 2.072 |
| Meng's [34] | $2T_{ST-FL}+2T_{FL-GS}$ | 0.009 |
| 本文方法 | $2T_{ST-FL}+2T_{CG-FL}$ | 0.278 |

第一部分为确定性交互时延, 即认证过程中一定会发生的交互过程所产生的时延, 包括端用户与转发面低轨卫星交互时延 $T_{ST-FL}$、控制面高轨卫星与转发面低轨卫星交互时延 $T_{CG-FL}$、控制面高轨卫星与地面站交互时延 $T_{CG-GS}$ 和转发面低轨卫星与卫星网络管理中心交互时延 $T_{FL-SN}$, 其中 $T_{FL-SN}$ 与 $T_{ST-FL}$ 相等, 根据文献[47]中链路时延, $T_{ST-FL}$ 约为 3 毫秒, $T_{CG-FL}$ 为 136 毫秒。另外, 由于控制面高轨卫星将认证响应同时发送给地面站和端用户, 因此控制面高轨卫星与地面站之间的交互时延 $T_{CG-GS}$ 不计入交互时延。

另一部分为非确定性交互时延, 即由于端用户到地面控制中心无确定链路而产生的星间转发时延 $T_{forward}$ 和星间路由计算更新时延 $T_{compute}$。转发次数记为 $m$, 由于卫星轨道可预测, 执行一次转发星间路由计算更新 1 次, 则非确定性交互时延可计算为 $m\cdot 2T_{forward}+T_{compute}$。根据文献[48]中的路由计算与更新估计值, $T_{compute}$ 平均值为 60 毫秒, 星间转发采用微波链路, 微波链路带宽为 2kbps, 星间距离为 1500 公里, 每传输 1($m$=1)次认证请求和响应, 转发传输时延约为 2 秒, 即 $2T_{forward}+T_{compute}$ 约为 2.06 秒。

根据以上认证时延的定义以及对比结果, 形成如下分析结果:

1) 根据表 4, 前三种方法均采用传统的卫星接入认证模型, 端用户直接与地面控制中心进行认证, 该方法以端用户可通过卫星链路连通地面控制中心为前提, 计算时延几乎可以忽略, 后两种方法的计算时延分别为 2.316 毫秒和 2.422 毫秒。

2) 根据表 5, 后两种方法均未采用传统的卫星接入认证模型, 而是采用星上认证的方法, 其中 Meng 等人[34]由低轨卫星代理地面站或者地面控制中心对端用户进行认证, 本文由控制面高轨卫星认证对端用户进行认证, 这两种方法虽然在计算时延方面相比较前三种方法增加了加法运算和乘法运算, 但是以上两种方法不以端用户与地面控制中心存在稳定链路为前提, 更符合实际的应用场景, 由表 5 的对比可以看到, 前三种方法的交互时延包含非确定性交互时延, 且该时延将随着端用户接入节点位置的变化而变化, 交互时延均为秒级, 而后两种方法不存在这种不确定性, 仅与地面段和空间段的距离相关, 交互时延均为毫秒级。

综上, 本文提出的方法在认证时延方面优于 Cheng 等人[29]、Liu 等人[43]以及 Lee 等人[28]提出的方法, 因此当端用户与地面控制中心不存在稳定链路时, 采用本文的模型以及方法认证时延更小。Meng 等人[37]和本文提出的方法相比较, 认证时延均为毫秒级, 在端用户可接受的范围内。

### 6.2 重认证时延

重认证时延定义为在低轨卫星过顶条件下, 端用户重新完成接入认证所需要的时间。该指标影响端用户访问空间服务的连续性。本文假设单位时间内有 $n$ 次低轨卫星过顶, 每次认证时间为 $T$, 由重认证所引起的延迟为 $n \cdot T$ 。

具体而言, Cheng 等人[29]、Liu 等人[43]Lee 等人[28]提出的方法未考虑卫星过顶场景, Meng 等人[34]提出的方法虽然考虑了低轨卫星过顶切换的场景, 但是该方法以低轨卫星与端用户之间的连接保持不变, 地面站与卫星之间的连接不断切换的假设为前提, 在实际环境中难以成立, 低轨卫星与端用户之间的连接无法持续保持, 根据低轨卫星行业研究报告, 平均约 4 分钟端用户就需要重新连接另外一颗低轨卫星, 若按照该频率, 一次会话的时间为 30 分钟, 由过顶所引起的重认证为 8 次, 若采用传统接入认证机制, 将额外引入 7 次重认证时延, 而本文提出的方法, 只需要在会话中进行一次认证, 不存在额外的重认证时延, 重认证开销仅为传统方法的 12.5%, 避免端用户频繁重复执行接入认证过程, 保证端用户访问空间服务的连续性。

综上, 本文提出的方法在重认证方面优于已有的方法。

### 6.3 认证算法计算时间开销

为了评估算法计算的时间开销, 本文进一步使用服务器(CPU 为 Intel core i5-2400, 主频 3.10GHz)搭建了实验环境, 端用户设备、控制面高轨卫星各使用一个虚拟机模拟(虚拟机均配置为单核, 内存 4GB)。使用 C 语言和 OpenSSL 库[49]实现端用户设备和控制面高轨卫星上的认证算法; 实验中, 椭圆曲线选择 secp265k1, 密钥长度为 256 位。为了保证实验结果的可靠性, 我们重复执行在本地认证算法 10000 次, 通过对 10000 次实验结果的统计分析, 得到如图 4 所示的三种计算开销 CDF 曲线。根据图 4 可知, 在合法端用户设备侧, 发起接入认证请求执行开销小于 2.289 毫秒的概率为 94.65%, 处理接入认证响应执行开销小于 1.628 毫秒的概率 96.14%; 在控制面高轨卫星侧, 处理接入认证请求执行开销小于 5.714 毫秒的概率为 90.25%。上述实验结果表明, 本文所提出的认证算法能够以毫秒级的开销应用在软件定义卫星接入认证环境中。

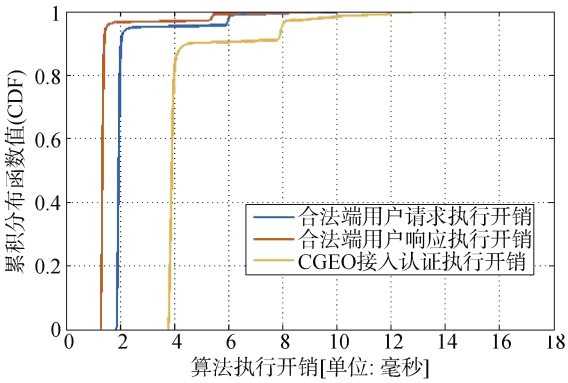


**图 4 执行开销累计分布函数图**

**Figure 4 The CDF of process time**

## 7 结论

本文提出了一种面向软件定义卫星网络的协同接入认证模型, 认证模型充分利用软件定义卫星网络具备管理面、控制面、转发面的分层结构特点, 将合法端用户设备的身份标识作为序参量, 建立了多层协同控制机制, 减少了软件定义卫星网络中接入认证服务所暴露的攻击面, 能够抵御针对接入认证的拒绝服务攻击; 基于该模型设计了空间网络拓扑动态高容忍的接入认证协议, 该协议利用地球同步轨道卫星具有全局视角、具备一定计算能力的特点, 确保合法端用户设备的在多星之间无感知切换, 保障访问的连续性。

通过数值分析和仿真实验, 在算法执行开销方面, 认证时延为毫秒级, 在端用户可接受的范围内, 同时, 切换过程无需端用户重新认证, 重认证开销降低了 81.5%。

综上，本文方法满足了卫星网络接入认证的一系列安全需求，并以更严格的方式实现了软件定义卫星网络的安全保护，且能够不降低用户体验，为软件定义卫星网络的接入认证技术的实现提供了借鉴。

## 参考文献


[1] Lasc I, Dojen R, Coffey T. Countering Jamming Attacks Against an Authentication and Key Agreement Protocol for Mobile Satellite Communications[J]. *Computers & Electrical Engineering*, 2011, 37(2): 160-168.

[2] Zheng G, Ma H T, Cheng C, et al. Design and Logical Analysis on the Access Authentication Scheme for Satellite Mobile Communication Networks[J]. *IET Information Security*, 2012, 6(1): 6.

[3] 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.

[4] Kapovits Á, Covaci S, Ververidis C, et al. Advanced Topics in Service Delivery over Integrated Satellite Terrestrial Networks[C]. *2014 7th Advanced Satellite Multimedia Systems Conference and the 13th Signal Processing for Space Communications Workshop*, 2014: 92-98.

[5] Bao J Z, Zhao B K, Yu W R, et al. OpenSAN: A Software-Defined Satellite Network Architecture[C]. *The 2014 ACM conference on SIGCOMM*, 2014: 347-348.

[6] Tang Z, Zhao B K, Yu W R, et al. Software Defined Satellite Networks: Benefits and Challenges[C]. *2014 IEEE Computers, Communications and IT Applications Conference*, 2015: 127-132.

[7] B. Barritt, and W. Eddy. SDN enhancements for LEO satellite networks[C]. *34th Aiaa International Communications Satellite Systems Conference*, 2016.

[8] Gardikis G, Costicoglou S, Koumaras H, et al. NFV Applicability and Use Cases in Satellite Networks[C]. *2016 European Conference on Networks and Communications*, 2016: 47-51.

[9] Gardikis G, Koumaras H, Sakkas C, et al. Towards SDN/NFV-Enabled Satellite Networks[J]. *Telecommunication Systems*, 2017, 66(4): 615-628.

[10] Ferrús R, Koumaras H, Sallent O, et al. SDN/NFV-Enabled Satellite Communications Networks: Opportunities, Scenarios and Challenges[J]. *Physical Communication*, 2016, 18: 95-112.

[11] Ferrus R, Sallent O, Ahmed T, et al. Towards SDN/NFV-Enabled Satellite Ground Segment Systems: End-to-End Traffic Engineering Use Case[C]. *2017 IEEE International Conference on Communications Workshops*, 2017: 888-893.

[12] Ferrus R, Koumaras H, Sallent O, et al. On the Virtualization and Dynamic Orchestration of Satellite Communication Services[C]. *2016 IEEE 84th Vehicular Technology Conference*, 2017: 1-5.

[13] Ahmed T, Ferrus R, Fedrizzi R, et al. Satellite Gateway Diversity in SDN/NFV-Enabled Satellite Ground Segment Systems[C]. *2017 IEEE International Conference on Communications Workshops*, 2017: 882-887.

[14] Ahmed T, Dubois E, Dupé J B, et al. Software-Defined Satellite Cloud RAN[J]. *International Journal of Satellite Communications and Networking*, 2018, 36(1): 108-133.

[15] Huang X Y, Zhao Z F, Meng X J, et al. Architecture and Application of SDN/NFV-Enabled Space-Terrestrial Integrated Network[M]. Communications in Computer and Information Science. Singapore: Springer Singapore, 2017: 244-255.

[16] Wang C F, Yu X S. Application of Virtualization and Software Defined Network in Satellite Network[C]. *2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 2017: 489-493.

[17] Shi L, Lu Z, Qin P, et al. OpenFlow Based Spatial Information Network Architecture[C]. *2015 International Conference on Wireless Communications & Signal Processing*, 2015: 1-5.

[18] Miao Y, Cheng Z J, Li W, et al. Software Defined Integrated Satellite-Terrestrial Network: A Survey[M]. Communications in Computer and Information Science. Singapore: Springer Singapore, 2017: 16-25.

[19] Sheng M, Wang Y, Li J D, et al. Toward a Flexible and Reconfigurable Broadband Satellite Network: Resource Management Architecture and Strategies[J]. *IEEE Wireless Communications*, 2017, 24(4): 127-133.

[20] Xu S, Wang X W, Huang M. Software-Defined Next-Generation Satellite Networks: Architecture, Challenges, and Solutions[J]. *IEEE Access*, 2018, 6: 4027-4041.

[21] Xue K P, Meng W, Zhou H C, et al. A Lightweight and Secure Group Key Based Handover Authentication Protocol for the Software-Defined Space Information Network[J]. *IEEE Transactions on Wireless Communications*, 2020, 19(6): 3673-3684.

[22] Zhang M H, Li G Y, Xu L, et al. Control Plane Reflection Attacks in SDNS: New Attacks and Countermeasures[M]. Research in Attacks, Intrusions, and Defenses. Cham: Springer International Publishing, 2018: 161-183.

[23] Cruickshank H S. A Security System for Satellite Networks[C]. *Fifth International Conference on Satellite Systems for Mobile Communications and Navigation*, 2002: 187-190.

[24] 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.

[25] Chang Y F, Chang C C. An Efficient Authentication Protocol for Mobile Satellite Communication Systems[J]. *ACM SIGOPS Operating Systems Review*, 2005, 39(1): 70-84.

[26] 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.

[27] 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 and Networking*, 2011, 2011(1): 1-10.

[28] 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 and Networking*, 2012, 30(1): 29-38.

[29] 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.

[30] Farash M S, Attari M A. An Efficient Client—Client Password-Based Authentication Scheme with Provable Security[J]. *The Journal of Supercomputing*, 2014, 70(2): 1002-1022.

[31] 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 and Networking*, 2014, 32(5): 443-452.

[32] G. Agapiou, F. Ferrús, A. Ramón, et al. SDN and NFV for satellite infrastructures[C]. *Institute of Electronics, Information and Communications Engineers*, 2016: 1-4.

[33] 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.

[34] Meng W, Xue K P, Xu J, et al. Low-Latency Authentication Against Satellite Compromising for Space Information Network[C]. *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems*, 2018: 237-244.

[35] Alagoz F, Gur G. Energy Efficiency and Satellite Networking: A Holistic Overview[J]. *Proceedings of the IEEE*, 2011, 99(11): 1954-1979.

[36] Vidal O, Verelst G, Lacan J, et al. Next Generation High Throughput Satellite System[C]. *2012 IEEE First AESS European Conference on Satellite Telecommunications*, 2013: 1-7.

[37] Mijumbi R, Serrat J, Gorricho J L, et al. Network Function Virtualization: State-of-the-Art and Research Challenges[J]. *IEEE Communications Surveys & Tutorials*, 2016, 18(1): 236-262.

[38] Hu Y R, Li V O K. Satellite-Based Internet: A Tutorial[J]. *IEEE Communications Magazine*, 2001, 39(3): 154-162.

[39] Yang Q Y, Xue K P, Xu J, et al. AnFRA: Anonymous and Fast Roaming Authentication for Space Information Network[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(2): 486-497.

[40] Bertaux L, Medjiah S, Berthou P, et al. Software Defined Networking and Virtualization for Broadband Satellite Networks[J]. *IEEE Communications Magazine*, 2015, 53(3): 54-60.

[41] Bu C, Wang X W, Cheng H, et al. Enabling Adaptive Routing Service Customization via the Integration of SDN and NFV[J]. *Journal of Network and Computer Applications*, 2017, 93: 123-136.

[42] Rossi T, De Sanctis M, Cianca E, et al. Future Space-Based Communications Infrastructures Based on High Throughput Satellites and Software Defined Networking[C]. *2015 IEEE International Symposium on Systems Engineering*, 2015: 332-337.

[43] Zhao W W, Zhang A X, Li J H, et al. Analysis and Design of an Authentication Protocol for Space Information Network[C]. *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 2016: 43-48.

[44] Ma D H, Xu Z, Lin D D. Defending Blind DDoS Attack on SDN Based on Moving Target Defense[M]. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham: Springer International Publishing, 2015: 463-480.

[45] Zhang R. *Research on certificateless public key cryptography based on ECC*[D]. Wuhan: Wuhan University, 2011.
(张瑞. 基于椭圆曲线密码的无证书公钥密码研究[D]. 武汉: 武汉大学, 2011.)

[46] Jia S P. *Research of certificateless anonymous multi-receiver signcryption based on ECC*[D]. Xi'an: Xidian University, 2018.
(贾生盼. 基于椭圆曲线的无证书匿名多接收者签密研究[D]. 西安: 西安电子科技大学, 2018.)

[47] Li T X, Zhou H C, Luo H B, et al. SERvICE: A Software Defined Framework for Integrated Space-Terrestrial Satellite Communication[J]. *IEEE Transactions on Mobile Computing*, 2018, 17(3): 703-716.

[48] Guo Q Z, Gu R T, Dong T, et al. SDN-Based End-to-End Fragment-Aware Routing for Elastic Data Flows in LEO Satellite-Terrestrial Network[J]. *IEEE Access*, 2018, 7: 396-410.

[49] OpenSSL libraries. https://www.openssl.org/docs/manmaster/man3/. Dec. 2022

**宋晨** 女, 硕士。中国科学院信息工程研究所高级工程师, CISSP。先后参与了发改委、科技部和中科院等国家及部委项目 10 余项, 获省部级科技进步一等奖一项。研究领域为网络安全、应用安全等。Email: songchen@iie.ac.cn

**王利明** 男, 博士。中国科学院信息工程研究所正高级工程师, 博导, CISSP, PMP。先后主持和参与了发改委、工信部、国新办等国家项目 20 余项, 申请专利 30 余项, 在国内外相关期刊或会议上发表论文 30 余篇。研究领域包括网络安全、云计算、数据安全等。Email: wangliming@iie.ac.cn

**徐震** 男, 博士。中国科学院信息工程研究所第五研究室主任, 正高级工程师, 中科院信息化规划咨询专家, 中国电子学会高级会员, 密码行业标准化技术委员会专家。研究领域为网络安全、智能设备安全等。曾主持十余项国家信息安全科技项目, 获省部级科技进步一等奖两项。Email: xuzhen@iie.ac.cn

**李宏佳** 男, 博士。中国科学院信息工程研究所副研究员, 硕导。先后主持或参与了国家自然科学基金、科技部等国家项目 10 余项, 已发表学术论文 60 余篇。研究领域为移动通信网络架构与安全防护等、MEC/边缘智能协同服务与数据隐私保护。Email: lihongjia@iie.ac.cn