

基于零信任的卫星互联网安全防护研究

宋宇飞¹, 周文辉², 刘建东¹, 李新鹏¹

(1.中国星网网络系统研究院有限公司, 北京 100029;

2.中国电子信息产业集团有限公司第六研究所, 北京 100083)

摘要: 卫星互联网作为“新基建”, 是我国未来信息基础建设的重要组成部分, 其安全重要性不言而喻。对零信任及零信任安全防护架构展开研究, 依据卫星互联网系统典型架构, 对卫星平台管控、卫星数据传输及卫星通信领域面临的安全风险进行分析, 针对上述风险, 提出基于零信任的卫星互联网安全防护架构, 并描述零信任安全防护架构在卫星管控、数据传输和通信典型应用场景中的实现过程, 及其与传统安全防护架构相比的优势。

关键词: 零信任; 卫星互联网; 零信任安全防护架构

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2021027

Research on Satellite Internet Security Protection Based on Zero Trust

SONG Yufei¹, ZHOU Wenhui², LIU Jiandong¹, LI Xinpeng¹

1.China Satellite Network System Institute Co.,Ltd., Beijing 100083, China

2.The 6th Research Institute of China Electronics Corporation, Beijing 100083, China

Abstract: Satellite internet, as a new infrastructure, is an important part of China's future information infrastructure, and its security importance is self-evident. Based on the typical architecture of satellite internet system, the security risks faced by satellite platform control, satellite digital transmission and satellite communication were analyzed, the satellite internet security protection architecture based on zero trust was put forward. The implementation process of zero trust security protection architecture in satellite control, digital transmission and communication typical application scenarios, and its advantages compared with the traditional security protection architecture were described.

Keywords: zero trust, satellite internet, zero trust security architecture

1 引言

卫星互联网利用庞大数量的低轨卫星作为“空中基站”, 支持通信、遥感、导航等多种业务, 具有速度快、带宽高、时延小的特点, 能够实现全球范围内立体化、全天候和全地域^[1]的万物互联, 消除“数字鸿沟”。

2020年4月, 国家发展和改革委员会首次明确新型基础设施范围, 卫星互联网被纳入“新基建”范畴。卫星互联网建成后, 可在移动通信、5G融合、宽带接入、物联网、导航增强和遥感监视等应用领域发挥重大作用, 为实施国家重大战略、确保国家信息安全、形成弹性空间体系、促进经济

社会发展、应对网络霸权主义等提供有力的战略支撑。

网络空间安全是社会服务和治理之基^[2], 卫星互联网安全作为其组成部分, 重要性不言而喻。有别于传统地面网络和高轨卫星通信系统, 卫星互联网存在卫星网络节点庞大、管控信道开放、拓扑结构高度变化、星上网络与地面网络互联互通等特点。现有互联网安全技术并不完全适用于卫星互联网, 而以往隐形信任链的卫星通信加密保护方式也不适用于卫星节点结构复杂且开放的卫星互联网, 因此急需一种细粒度、持续动态、最小权限的安全防护架构。

2 卫星互联网系统典型架构

卫星互联网由空间段、地面段和用户段3部分组成^[3],其中空间段由低轨卫星平台组成;用户段由各种用户站构成,可分为固定用户站和移动用户站^[4];地面段包含各类测控站、卫星测控中心、各类信关站以及运维管控中心等。用户站与卫星建立用户链路,通过切换控制和空地协议转换为用户终端提供接入卫星通信服务。测控站和测控中心负责实现对卫星节点位置、姿态、星历表的管理。信关站集成了LTE核心网中移动管理实体(Mobility Management Entity, MME)、服务网关(Serving Gateway, S-GW)、分组数据网络网关(Packet Data Network Gateway, P-GW)、策略和计费规则功能(Policy and Charging Rules Function, PCRF)等模块的功能^[5],负责指向跟踪、信号收发、受控切换、流量控制、路由寻址,以及对卫星及用户资源的管理。运维管控中心对各个模块进行统一管理和调度,是整个系统的控制中枢^[4]。

卫星互联网架构示意如图1所示。

3 卫星互联网面临的安全风险

3.1 低轨卫星管理安全风险

结合卫星互联网系统架构,对其面临的安全风险进行分析。

低轨卫星作为卫星互联网“新基建”的核心基础设施,其安全防护是整个卫星互联网正常运行的重中之重。低轨卫星的管理由测控站、测控中心、信关站及运维管控中心共同参与,涉及卫星平台测控和卫星载荷测控。

传统测控安全系统主要针对对外部对卫星遥控指令的破译、篡改和重放等攻击进行防护,防止卫星出现关闭、变轨、载荷失控等异常情况。卫星互联网作为商用信息服务系统和国家重要基础设施,其运营和管理由多个地面段设施和多个管理方共同参与,有些设施甚至可能处于境外,且管理设备和管理人员复杂,依靠管理制度和个人安全意识实现对内外部攻击防护和权限管理漏洞填补的方式是不可靠的。

例如内部人员通过窃取身份认证密钥和登录口令,获得卫星遥控指令发送设备的控制权,可以向测控网络发送非法操作指令。此外,获得合法卫星遥控指令发送设备控制权的内部人员,其操作权限范围和操作时间也是不可控的,攻击者可利用合法控制人员不在的间隙,向卫星发起攻击。

3.2 卫星数据传输安全风险

未来卫星互联网不仅在卫星通信方面发挥作用,随着卫星遥感服务多元化,利用无线电掩星、微波探测、

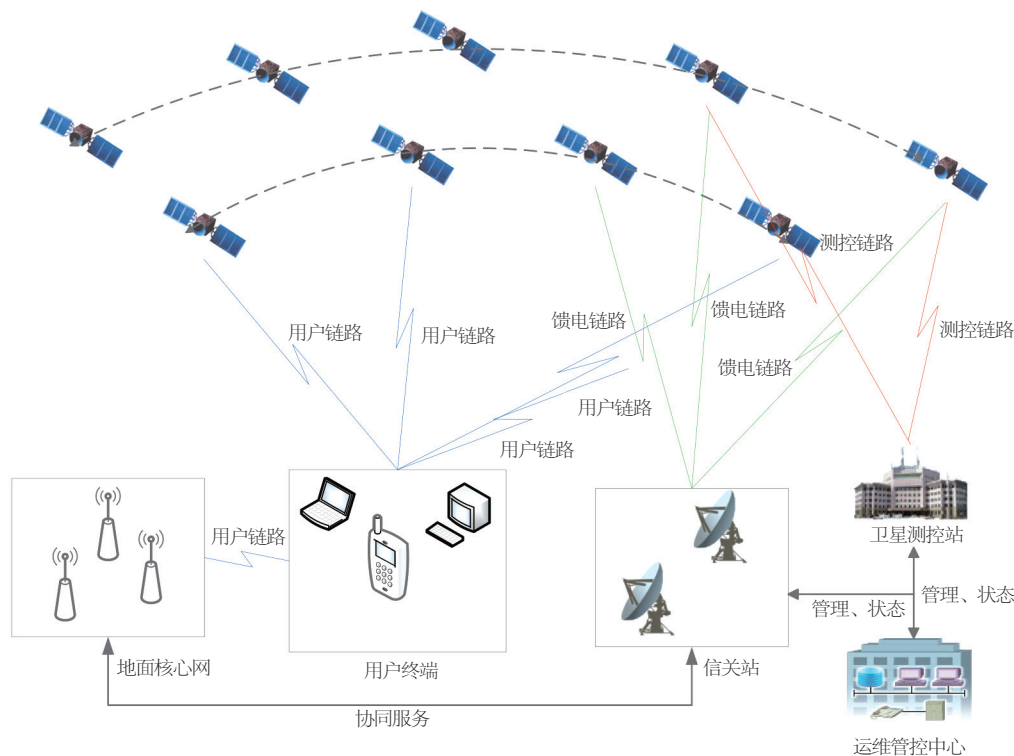


图1 卫星互联网架构示意

光学探测和电子探测等手段获得数据的能力越来越成熟,进一步推进卫星数据传输服务成为卫星互联网的一大核心业务。

传统卫星传输数据采用端到端的加密,且由于应用范围的限制未对访问者身份权限进行细致甄别,是一种隐式信任链。而卫星互联网的载荷数据作为一种高价值数据,可在政府管理、气象监测、环境保护、科技创新及交通运输等多领域使用,不再存在隐式信任关系,因此其合法权益获取和数据传输过程保护显得极为重要。

非法用户可以通过对卫星互联网运维管控中心或信关站的攻击,伪造冒充合法用户,获取操作权限和数据解密密钥,进而向低轨卫星发送数据下载请求,利用卫星接收终端接收、传输数据并解密,造成数据泄露。

另外合法访问者可以获取远大于其需求的数据资源,进而利用某一数据访问权限的漏洞迅速扩展获取其他重要数据,造成重要数据资源的泄露。

3.3 卫星通信安全风险

卫星通信是卫星互联网最主要的业务。目前卫星互联网可通过信关站或地面专用通信终端与地面核心网连接。与地面网络的融合,将导致接入节点种类数量增多,自主通信链路增加,用户层级多样化发展,个人移动终端、固定终端和智能终端都可在任何时间、任何地点使用卫星互联网进行远程数据传输。此外卫星互联网通信业务不仅涉及普通大众全球通信服务,还涉及国家众多关键基础设施的数据传输和远程控制服务,如在能源、水利、交通等领域。但卫星互联网众多卫星及配套通信设备使用现成的商用技术来降低成本,零部件由多厂商提供,通信接入设备权限管理混乱、接入设备安全性参差不齐以及接入程序存在漏洞等情况将对卫星互联网通信带来极大风险。

卫星互联网系统具有天然的跨境覆盖和全球通信特性,境内信关站可以直接管理,但境外信关站和一些可以直接接入卫星的小型终端存在较大管理难度,攻击者可以低成本伪造卫星接收终端,很容易截获卫星通信的传输信号,从而破解数据。通过专业的信号分析,监听者可以解析整个卫星系统的通信编码体制,从而使该卫星系统“裸奔”。

卫星互联网作为天基通信网络,同样面临着网络攻击的风险。2018年6月,安全企业赛门铁客(Symantec)发布报告^[6],称黑客组织可能正在谋求对卫星实施网络攻击。也有其他研究报告^[7]显示,针对卫星系统利用接收途径和各种软硬件所存在的“后门”漏洞,通过欺骗等网络攻击手段,可以使星载工作设备陷入间歇性或全面性

瘫痪。上述网络攻击,不仅会对卫星互联网系统的服务造成影响,还可能给用户的重要数据带来泄密、丢失或篡改的风险^[8],进而造成重大损失。

卫星互联网不仅是国家重要信息基础设施,也是国防战略发展的重要利器,尤其可以在自然灾害、战时等极端情况下进行全球信息传输。因此,卫星互联网一旦出现安全隐患并被敌对势力利用,将对我国国家安全带来巨大的威胁。

低轨互联网作为“新基建”,在卫星自身管理、载荷数据获取、卫星通信和设备、用户、应用传输等方面面临来自内部和外部多方面安全风险,所有内外部接入设备、用户都可伪造认证,骗取授权,从而达到攻击卫星互联网的目的。本文通过设计一种基于零信任安全架构的卫星互联网通信系统安全建设方案,提高卫星互联网空间通信系统的安全防护能力。

4 零信任及零信任安全防护架构概念

“零信任”(Zero Trust, ZT)未出现之前,其概念就一直应用于网络安全中,美国国防信息系统局(DISA)和国防部(DOD)公布了一种从边界的安全模型转移到关注单个事物安全的模型,并称之为“Black Core”。随着去边界化概念的不断演进,“零信任”逐渐浮出水面,John Kindervag在Forrester创立了“零信任”一词。2020年8月,美国国家标准技术研究院(NIST)给出了零信任架构(Zero Trust Architecture, ZTA)的抽象定义和一般部署模型及用例。

零信任是一种以资源保护为核心的网络安全范式,其前提是信任从来不是隐式授予的,而是必须进行持续评估的。零信任架构是利用零信任概念,并囊括内部组件关系、工作流程和访问策略的一种安全规划。零信任安全总体架构示意如图2所示。

零信任架构有3个基本要素:主体、客体、数据流。主体包括用户、设备、应用等接入系统的各类要素;客体包括功能、服务、数据等主体要访问或操作的各类要素;数据流为主体与客体之间数据交互的数据流量。

零信任架构用于处理主体、客体及数据流量的方式借鉴了网络系统经常使用的概念,将用于控制、配置网络的数据流和用于执行实际应用的数据流隔离开来。这种隔离通常可分为控制平面和数据平面。零信任架构中的数据平面处于数据传输路径上,需控制平面决定数据传输链路的通断;控制平面由一系列组件构成。这些组件接收并处理来自数据平面的请求,检查发起请求的主体的相关数据,以确定该访问主体是否可信。控制平面一旦做出授权判断,就会通知或者重新配置数据平面,

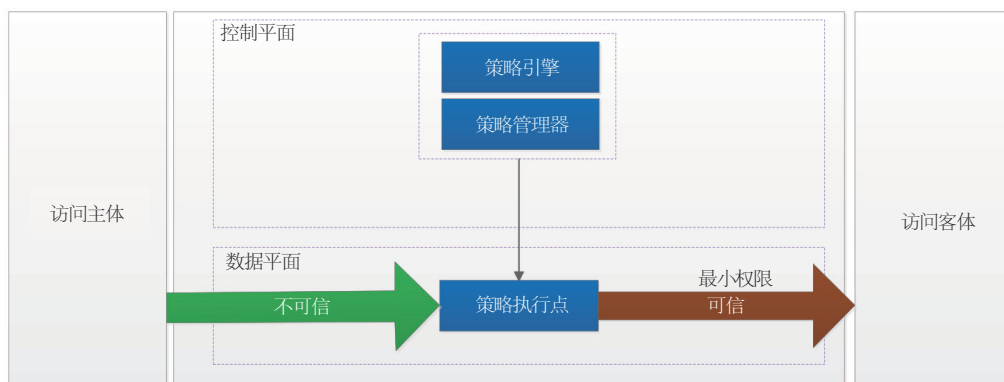


图2 零信任安全总体架构示意

并授予其相应的访问权限。

核心组件由下列要素组成。

(1) 策略引擎 (PE)：该组件部署于控制平面，负责决定是否授予特定访问主体对资源的访问权限。策略引擎使用系统安全策略及外部安全策略的输入作为“信任算法”的输入，以决定授予、拒绝或撤销对该资源的访问权限。

(2) 策略管理器 (PA)：该组件部署于控制平面，负责建立/切断主体与资源之间的通信路径。它将生成具体会话的身份验证令牌或凭证，供访问主体使用。它与策略引擎密切相关，并依赖策略引擎做出允许或拒绝会话的决定。

(3) 策略执行点 (PEP)：该组件部署于数据平面，负责启用、监控并最终结束访问主体和资源之间的连接。策略执行点是零信任架构中的逻辑组件，在实际应用中可以分为两个不同的物理组件：一个部署于访问

主体端，另一个部署于资源段。

5 卫星互联网零信任安全架构

借鉴上述零信任安全架构，卫星互联网零信任安全架构由访问主体、访问客体、零信任安全组件及身份安全基础设施4部分组成。

卫星互联网零信任安全架构中，访问主体是访问设备与用户数字身份信息整合后的实体；访问设备包括运营设备、管控设备、通信终端、数据终端等。访问客体是需要保护的资源，包括卫星载荷和卫星平台的管控指令、卫星载荷数据、地面和卫星的通信信令、卫星通信数据等。

卫星互联网零信任安全架构的安全组件分别部署于控制平面和数据平面。其中控制平面包含策略引擎和策略管理器，数据平面包含策略执行点。卫星互联网零信任安全架构如图3所示。

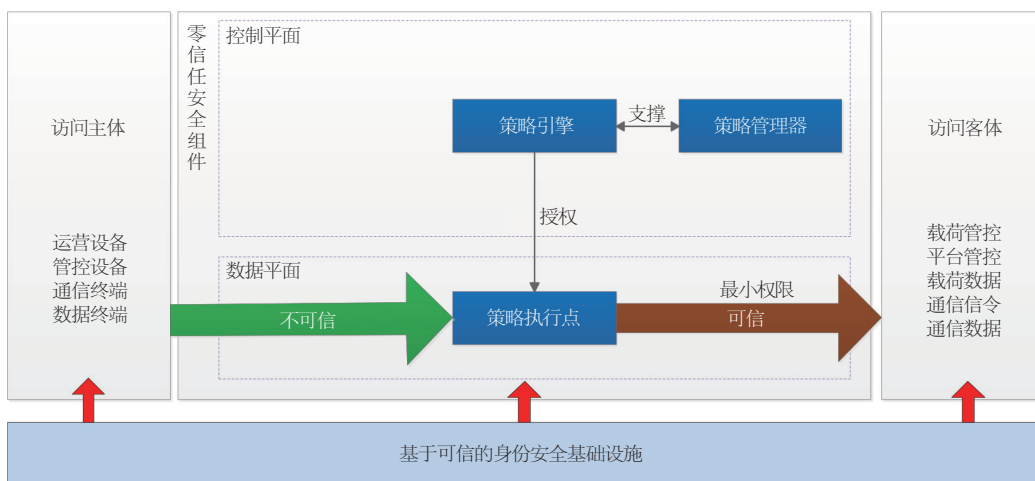


图3 卫星互联网零信任安全架构

5.1 建立初始信任

访问主体在访问前需具备基础信任信息。这些信息包含访问设备自身、设备所处环境及使用用户的参数信息。基础信任信息的真实可靠是实现卫星互联网零信任安全防护架构的前提,通过预先配置的可信单元实现对访问主体设备自身软件和固件的验证,防止主体设备操作系统、底层驱动及应用软件被人篡改,确保认证过程中的基础信任信息真实可靠。

基础信任信息中设备自身的参数信息 M 包括设备编号 D_{ID} 、可信根编号(TC_N)及可信根密钥 TC_k 的哈希运算,参数信息 M 按照式(1)获取

$$M = D_{ID} \parallel TC_N \parallel \text{Hash}(TC_k) \quad (1)$$

设备所处环境信息 D_E 由终端环境感知系统获取;使用用户基础信任信息 U_M 需提供用户位置信息 U_L 、用户 U_{ID} 的哈希值、所属组织机构信息 U_I 、邮箱信息 U_E 及地址信息 U_A 等信息,按照式(2)获取。基础信任信息 M_F 按照式(3)获取。

$$U_M = U_L \parallel \text{Hash}(U_{ID}) \parallel U_I \parallel U_E \parallel U_A \quad (2)$$

$$M_F = M \parallel D_E \parallel U_M \quad (3)$$

用户将访问请求 AQ_M 和基础信任信息 M_F 利用策略管理器所提供的公钥 PU_{PA} 进行加密保护。策略引擎输入信息 I_M 加密保护按照式(4)进行。

$$I_M = E(PU_{PA}, (AQ_M \parallel M_F)) \quad (4)$$

5.2 策略管理器

策略管理器是对策略引擎的支撑,直接影响授权的决策。策略管理器包含私有公钥基础设施、身份管理系统、数据访问策略、安全态势组件、安全信息事件管理和威胁情报源。

(1) 私有公钥基础设施

私有公钥基础设施为策略引擎提供证书服务,访问主体的访问请求 AQ_M 和基础信任信息 M_F 都必须利用该私有公钥基础设施所提供的公钥 PU_{PA} 进行传输加密保护。

(2) 身份管理系统

身份管理系统负责创建、存储和管理系统访问主体的身份信息,包括设备自身的参数信息 M 和使用用户基础信任信息 U_M 及对应访问主体拥有的最高权限等级。

(3) 数据访问策略

数据访问策略根据卫星互联网系统对载荷管控、平台管控、载荷数据服务、通信信令控制和通信业务服务的操作权限和使用范围进行预先制定。默认对卫星互联网系统划分5个等级的主体访问权限,访问客体与访问主体权限等级对应关系见表1。随着后续实际使用需求的增加,可在原有数据访问策略上进行迭代更新。

表1 访问客体与访问主体权限等级对应关系

序号	访问客体	访问主体权限等级
1	平台管控	A
2	载荷管控	A、B
3	载荷数据服务	A、B、C
4	通信信令控制	A、B、C、D
5	通信业务服务	A、B、C、D、E

(4) 安全态势组件

安全态势组件收集卫星互联网星座测运控链路、馈电链路、用户链路及地面链路所涉及的访问主体和客体设备可信单元的运行状态及所处环境信息,并将该态势信息存储记录,供威胁情报源进行分类运算。

(5) 安全信息事件管理

安全信息事件管理收集系统已发生的安全事件信息,如测控链路遭受重放攻击、通信信令被篡改、服务超时及越权申请等安全事件,并对该攻击事件所涉及的链路访问主客体设备基础信任信息进行记录,记录数据供威胁情报源进行分类运算。

(6) 威胁情报源

威胁情报源可利用身份管理系统、安全信息事件管理和安全态势组件提供的特征数据对访问主体进行分类计算,计算结果作为策略引擎算法的输入参数。安全信息事件管理特征数据包含超时访问、越权操作以及重放、篡改等攻击;安全态势组件特征数据包含当前设备私钥管理、部署位置、工作状态、主备状态、软件版本等信息。威胁情报源的分类算法是策略管理器的核心部分,由于该分类算法特征值为离散随机变量,预测结果为类别,且具有不连续、多输出等特点,宜采用决策树(Decision Tree)分类算法进行威胁情报源预测。

5.3 策略引擎

策略引擎是持续动态地对访问主体进行身份认证和授权,不存在“一劳永逸”的认证;同时策略引擎对访问主体的授权遵循最小权限原则,只授予完成任务所需权限,而不是授予访问主体想要的权限。策略引擎内部单元结构如图4所示。

策略引擎是零信任安全架构中的授权决策组件,利用策略管理器私有公钥基础设施获取对输入信息 I_M 进行解密的私钥 PR_{PA} ,解密后将 I_M 转发给策略管理器。策略管理器根据输入信息 I_M 将威胁情报源的结果数值作为策略管理器支撑信息 S_M 输出给策略引擎。

策略引擎的信任算法基于分值来计算每个访问主体

的权重。如果分值大于所配置资源阈值，则授予访问权限，否则请求被拒绝。分值根据访问主客体之间的 S_M 进行计算。信任算法首先获取用户的访问请求 AQ_M 和基础信任信息 M_F ，并从策略管理器的数据访问策略中进行匹配计算得到初始评分；随后利用基础信任信息 M_F 获取的威胁情报源分类结果计算得到二次评分，将最终评分传递至权限评估；权限评估后由信任算法输出主客体交互

所需的对称算法密钥、交互有效时间戳及相应访问主体权限等级参数。策略引擎工作原理如图5所示。

5.4 策略执行点

策略执行点为基于可信计算且具有密码运算功能的硬件计算单元或设备。策略执行点部署于访问主体和访问客体，接收策略引擎的管理，负责完成访问主体和访

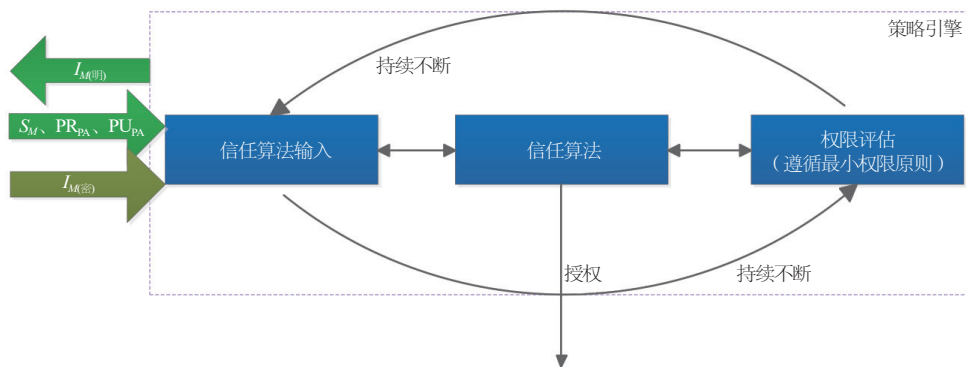


图4 策略引擎内部单元结构

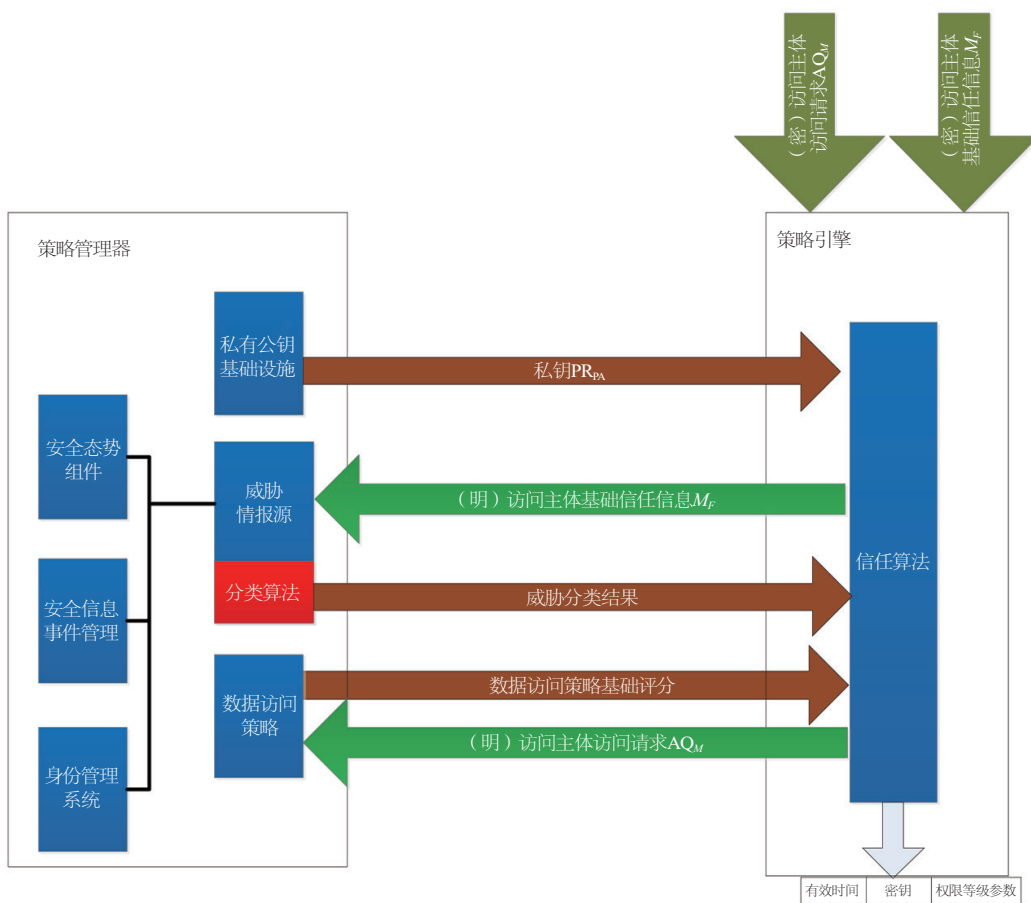


图5 策略引擎工作原理

问客体间数据平面链路的通断控制以及传输过程的加密保护。

6 卫星互联网零信任安全防护架构典型应用场景

卫星互联网通信时需通过载荷遥控指令实现对卫星通信载荷的调整,其面临的安全风险如3.1小节所述。传统卫星载荷遥控和平台遥控都由测控中心负责,默认指令产生和指令发送端均安全可靠,实行点对点的遥控传输加密。卫星互联网中卫星数量庞大,管控需求频繁,可攻击漏洞较多,除外部攻击的威胁,更多需防范来自内部或由外入内的攻击。利用零信任安全防护架构全方位地对载荷遥控申请、产生和发送端进行管控,有助于对载荷安全、可靠、高效的管理。

卫星互联网零信任安全架构卫星通信载荷控制指令应用场景如图6所示。策略管理器和策略引擎部署于卫星互联网运维管控中心;策略执行点基于可信计算分别部署于访问主体(信关站)和访问客体(低轨卫星)。信关站发送服务请求申请对卫星载荷的控制,该服务请求在数据平面建链传输前,需经过策略引擎授权,减弱内部攻击的可能性。信关站首先申请运维管控中心的公钥证书,利用该公钥向运维管控中心的策略引擎发送载荷指令来传递服务请求和身份认证请求;策略管理器利用访问主体的基础信任信息和请求信息对其身份进行验证、分级并给出初始访问策略,并对其是否属于威胁源进行分类。策略引擎利用策略管理器支撑信息实现对访

问主体身份的认证、权限的分级和使用时间的划分,并最终将数据平面使用的对称算法密钥分别下发给信关站和低轨卫星的策略执行点,本次授权结束。信关站与低轨卫星利用双方的策略执行点实现空中接口数据链路的传输加密,并由低轨卫星接收载荷遥控指令并执行。

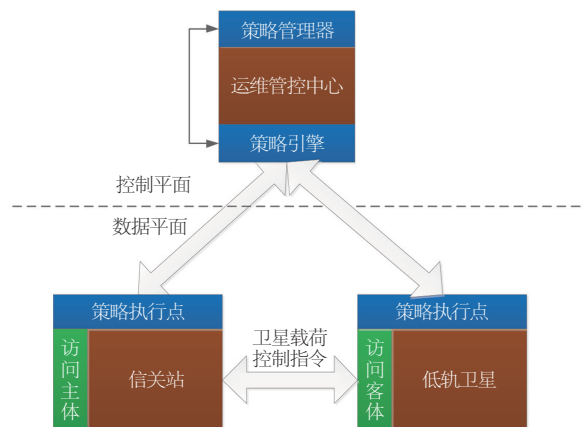


图6 卫星互联网零信任安全架构卫星通信载荷控制指令应用场景

卫星互联网通信用户端可获取通信服务。低轨卫星通信过程面临的安全风险如3.3小节所述,传统卫星通信终端在入网后默认该通信终端安全可靠,利用密钥分配中心(Key Distribution Center, KDC)实现对通信双方密钥的分发,后续不再对用户终端进行认证。但卫星互

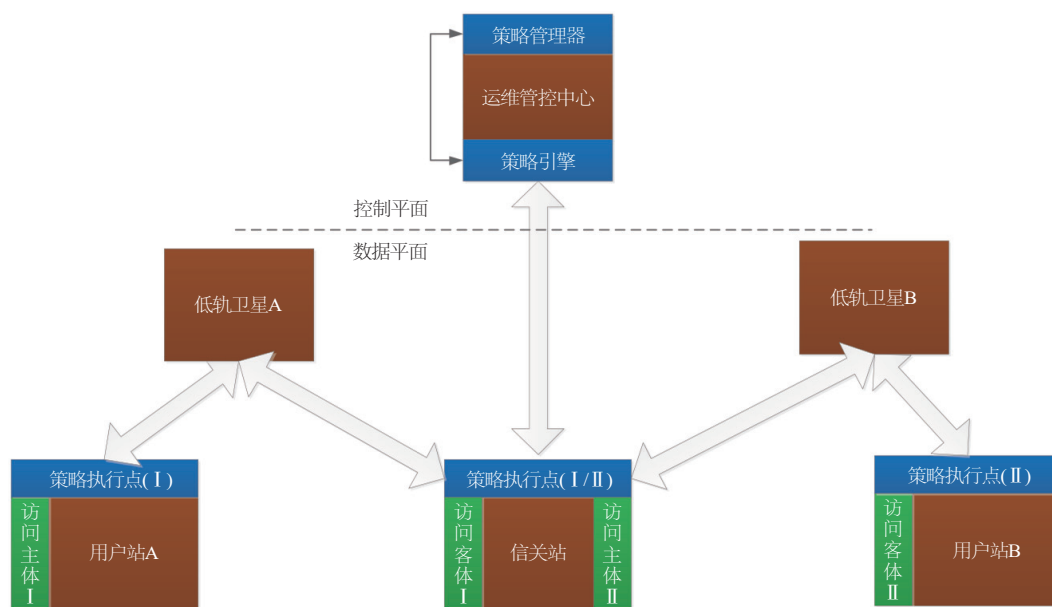


图7 卫星互联网零信任安全架构卫星通信应用场景

联网用户终端境内外均有部署、所处环境复杂、使用者身份不再固定、各用户使用权限不同都带来诸多安全隐患。利用零信任安全防护架构可有效解决上述问题,提升卫星互联网通信系统的安全防护能力。

卫星互联网零信任安全架构卫星通信应用场景如图7所示。以低轨卫星双跳通信类型为例,策略管理器和策略引擎部署于卫星互联网运维管控中心,策略执行点基于可信计算分别部署于运维管控中心、用户站A、用户站B和信关站。用户站A发送通信服务请求,该服务请求在数据平面建链传输前,需经过策略引擎授权。用户站A通过信关站中转,并最终完成与用户站B的通信。用户站A与用户站B正式通信前,信关站首先向运维管控中心申请运维管控中心自身公钥证书,利用该公钥证书向运维管控中心发送服务请求及身份认证请求。信关站服务请求和身份认证请求通过后,信关站将转发用户站A向运维管控中心公钥证书获取请求,用户站A利用该公钥经信关站向运维管控中心的策略引擎发送通信服务获取请求和身份认证请求。策略管理器利用访问主体的基础信任信息和请求信息对其身份进行验证、分级并给出初始访问策略,对其是否属于威胁源进行分类。策略引擎利用策略管理器支撑信息实现对访问主体身份的认证、权限的分级和使用时间的划分,完成数据平面用户站A和信关站通信使用的对称算法密钥的分发,以及信关站和用户站B通信使用的对称算法密钥的分发,本次授权结束。用户站A与用户站B及信关站的策略执行点实现通信数据链路的传输加密,并完成用户站A与用户站B的通信服务。

7 思考与展望

零信任作为新的安全理念,可应用于卫星互联网的安全防护体系中,通过身份认证、权限管控、持续评估等多种技术,实现细粒度、多层级、精准化的访问控制,有效实现对载荷管控、平台管控、载荷数据、通信信令、通信数据的内外部安全威胁的防范。目前零信任安全防护架构已然在大数据、云计算、物联网和5G等场景下实现了技术突破,在卫星互联网领域还尚无有效、成熟的解决方案。希望本文能够对未来卫星互联网零信任安全防护架构解决方案的应用起到有效的推动作用。未来零信任安全防护架构在卫星互联网的落地仍需在政策、技术、推广等方面继续努力。

参考文献:

[1] 李力,戴阳利. “新基建”背景下卫星互联网发展的机遇和风

险[J]. 卫星应用, 2020(8): 38-42.

LI L, DAI Y L. Opportunities and risks of satellite Internet development under the background of "new infrastructure" [J]. Satellite Application, 2020(8): 38-42.

[2] 李风华. 信息技术与网络空间安全发展趋势[J]. 网络与信息安全学报, 2015, 1(1): 8-17.

LI F H. Development trends of the information technology and cyberspace security[J]. Chinese Journal of Network and Information Security, 2015, 1(1): 8-17.

[3] 陆洲, 秦智超, 张平. 天地一体化信息网络系统初步设想[J]. 国际太空, 2016(7): 20-25.

LU Z, QIN Z C, ZHANG P. Initial layout of space-ground integrated information network system[J]. Space International, 2016(7): 20-25.

[4] 徐超男, 张勇, 郭达, 等. 低轨卫星通信系统网络设计[J]. 通信技术, 2017, 50(9): 1942-1947.

XU C N, ZHANG Y, GUO D, et al. Network design of LEO satellite communication system[J]. Communications Technology, 2017, 50(9): 1942-1947.

[5] ZHANG Z. Performance simulation research of LTE star earth fusion network based on NS-3[D]. Xi'an: Xi'an Electronic and science University, 2015.

[6] 李风华, 张林杰, 陆月明, 等. 天地网络安全保障技术研究[J]. 天地一体化信息网络, 2020, 1(1): 17-25.

LI F H, ZHANG L J, LU Y M, et al. Research on space-ground network security guarantee technology[J]. Space-Integrated-Ground Information Networks, 2020, 1(1): 17-25.

[7] 邓招, 张晓玉. 太空中的网络安全问题[J]. 网络空间安全, 2017, 8(S5): 1-6.

DENG Z, ZHANG X Y. Network security problems of space[J]. Cyberspace Security, 2017, 8(S5): 1-6.

[8] 彭长艳. 空间网络安全关键技术研究[D]. 长沙: 国防科学技术大学, 2010.

PENG C Y. Research on key security technologies in space networks[D]. Changsha: National University of Defense Technology, 2010.

[9] COONEY M. IBM embraces zero trust with upgraded Cloud Pak service[J]. Network World (Online), 2021.

[10] BAKSH M. NSA pushes zero trust principles to help prevent sophisticated hacks[J]. Nextgov Com (Online), 2021.

[11] 孙晨华. 天基传输网络和天地一体化信息网络发展现状与问题思考[J]. 无线电工程, 2017, 47(1): 1-6.

SUN C H. Research status and problems for space-based transmission network and space-ground integrated information

network[J]. Radio Engineering, 2017, 47(1): 1-6.

- [12] 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.

- [13] EVAN G, DOUG B. Zero Trust Networks: Building Security System in Untrusted Network[M]. BeiJing: Posts and Telecommunication Press, 2019.

- [14] JASON G, JERRY W C. Zero Trust Security[M]. [S.l.:s.n.], 2021.

- [15] DHAR S, BOSE I. Securing IoT devices using zero trust and blockchain[J]. Journal of Organizational Computing and Electronic Commerce, 2021, 31(1): 18-34.

- [16] 章小宁, 朱立东. 通信与安全一体化的天地异构融合网络体系架构[J]. 天地一体化信息网络, 2020, 1(2): 11-16.

ZHANG X N, ZHU L D. Communication and security integrated space-earth heterogeneous network architecture[J]. Space-Integrated-Ground Information Networks, 2020, 1(2): 11-16.

[作者简介]



宋宇飞 (1991-), 男, 硕士, 中国星网网络系统研究院有限公司高级工程师, 主要研究方向为信息安全保密。



周文辉 (1973-), 男, 硕士, 中国电子信息产业集团有限公司第六研究所高级工程师, 主要研究方向为卫星通信保密。



刘建东 (1974-), 男, 硕士, 中国星网网络系统研究院有限公司高级工程师, 主要研究方向为信息安全保密。



李新鹏 (1975-), 男, 硕士, 中国星网网络系统研究院有限公司高级工程师, 主要研究方向为网络安全。