

# 天地一体化网络安全使能技术研究

## Research on Security Enabling Technologies of Space-ground Integrated Network

王蕴实<sup>1,2</sup>,张曼君<sup>1,2</sup>,徐雷<sup>1,2</sup>,谢中怀<sup>1,2</sup>(1. 中国联通研究院,北京 100048;2. 下一代互联网宽带业务应用国家工程研究中心,北京 100048)

Wang Yunshi<sup>1,2</sup>,Zhang Manjun<sup>1,2</sup>,Xu Lei<sup>1,2</sup>,Xie Zhonghuai<sup>1,2</sup>(1. China Unicom Research Institute, Beijing 100048, China; 2. Next Generation Internet Broadband Service Application National Engineering Research Center, Beijing 100048, China)

### 摘要:

多样化的场景、接入方式以及新型网络架构,给天地一体化网络安全带来了新的需求和挑战。从梳理天地一体化网络新特征入手,提出了天地一体化网络安全新挑战;分析了天地一体化网络在认证鉴权、数据传输和攻击溯源方面的安全风险和需求,并探讨了应对相关问题的天地一体化安全使能技术。

### 关键词:

天地一体化;安全;使能技术

doi:10.12045/j.issn.1007-3043.2023.08.001

文章编号:1007-3043(2023)08-0001-04

中图分类号:TN915.08

文献标识码:A

开放科学(资源服务)标识码(OSID):



### Abstract:

Diversified scenarios, diversified access modes and new network architecture bring new demands and challenges to the space-ground integrated network security. Starting from sorting out the new features of the space-ground integrated network, new challenges to the space-ground integrated network security are proposed. The security risks and requirements of authentication, data transmission and maintenance, and attack traceability are analyzed. The enabling technologies of space-ground integrated network security to solve related problems are discussed.

### Keywords:

Space-ground integrated networks; Security; Enabling technologies

引用格式:王蕴实,张曼君,徐雷,等. 天地一体化网络安全使能技术研究[J]. 邮电设计技术,2023(8):1-4.

## 0 引言

随着卫星通信技术的发展,卫星通信网络与地面通信网络在体制和技术上已基本具备融合的条件。天地一体化网络是以地基网络为基础,天基网络为补充和延伸,对空、天、地、海多场景统一服务,全球无缝立体覆盖的信息通信网络,具有重要的经济效益和社会效益。

### 1 天地一体化网络发展机遇

随着天地一体化网络军用价值被广泛关注和其商业价值的不断提升,全球各国愈发重视天地一体化

网络的战略地位及产业建设,全球在轨卫星数量稳步增长,且呈现低轨化、小体量化发展趋势。美国政府推出《国家航天战略》,通过部署多个卫星星座计划,推进低轨通信卫星组网工程建设,力争主导全球低轨宽带卫星市场。欧盟通过 IRIS2 卫星网络,为其提供宽带卫星网络服务,用于军事、政府与公众用途。我国也非常重视天地一体化网络的发展,工信部《“十四五”信息通信行业发展规划》中强调加强卫星通信顶层设计和统筹布局,推动高轨卫星与中低轨卫星协调发展。推进卫星通信系统与地面信息通信系统深度融合,初步形成覆盖全球、天地一体的信息网络。天地一体化网络迎来重大发展机遇,关于天地一体化网络的研究已经全面展开,并吸引了学术界和产业界的关注。多样化的场景、接入方式以及新型网络架构,

收稿日期:2023-06-16

给天地一体化网络安全带来了新的需求和挑战,推进天地一体化网络安全技术的发展刻不容缓。

## 2 天地一体化网络安全新挑战

天地一体化网络相比传统移动通信网络发生很大变化,呈现出物理环境复杂化、网络架构异构化、多协议栈融合化和跨域互联规模化的新特征<sup>[1-4]</sup>。这种天地一体化网络新特征也带来新的安全挑战。

a) 物理环境复杂化。天地一体化网络部署的物理环境进一步复杂化与开放化,网络基础设施面临自然环境破坏、信号干扰<sup>[5]</sup>、星上安全防护困难等挑战,影响设备的可用性。

b) 网络架构异构化。天地一体化网络跨越陆、海、空、天多层级建设形成融合网络,对网络安全要求进一步提高,需要部署适用于融合网络的安全功能,抵抗网络安全风险。

c) 系统协议融合化。天地一体化网络多系统多协议栈融合,需要对卫星部署网络和地面部署网络进行统一安全管理,实行星地融合、协同联动的安全运维和防护。

d) 跨域互联规模化。天地一体化多域异构互联模式下,加剧数据安全风险,需要对天地一体化网络数据进行全生命周期安全管理,并根据上级监管要求,履行数据安全保护职责。

## 3 天地一体化网络典型安全风险和需求分析

天地一体化网络面临海量多源终端接入、跨域网元互联、传输信道开放变化、数据流转路径复杂等问题。需要重点关注认证授权安全、数据传输安全和跨域攻击溯源等方面的安全风险和安全需求。

a) 认证授权安全。天地一体化异构融合网络架构下,不同业务场景下不同对象具备差异化的安全认证需求,需要针对具体应用场景和安全需求选择合适的认证鉴权技术,保障天地一体化网络认证授权安全<sup>[6]</sup>。天地一体化网络需要在更广的覆盖范围内,支撑海量多源终端随时随地无缝安全接入异构融合网络,而天基节点资源受限,存在认证拥塞安全风险。卫星节点长期运行在暴露的空间轨道,且拓扑周期性高度动态变化,攻击者更易假冒、劫持合法网络节点,需要加强跨域互联网元的认证鉴权。同时,多运营方融合组网场景下,还需要满足多方互信需求。

b) 数据传输安全。天地一体化网络相比传统地

面网络面临传输信道开放、传输距离跨度大等问题,数据窃听和数据仿冒等安全威胁更加突出,数据传输安全风险加剧。需要持续关注天地一体化网络的无线链路数据传输安全风险、互联互通网元数据传输安全风险和OM数据传输安全风险等问题,利用成熟的安全措施、有效的安全手段、创新的安全技术来应对。

c) 跨域攻击溯源。天地一体化网络在政治、军事、经济、文化和社会等领域广泛应用的同时,国家间的对抗形势也日益严峻,空天地一体化网络攻防呈现出国家化、军事化、常态化的趋势,跨组织、跨地域、复杂多样的网络攻击,不仅对监测防御能力提出新的要求,更是为溯源追踪带来巨大挑战。

## 4 天地一体化网络安全使能技术研究

根据对天地一体化网络面临的安全风险和需求的分析,建议重点考虑将认证鉴权安全技术、数据传输安全技术、跨域攻击溯源技术应用于天地一体化网络规划、建设、运营工作中(见图1)。

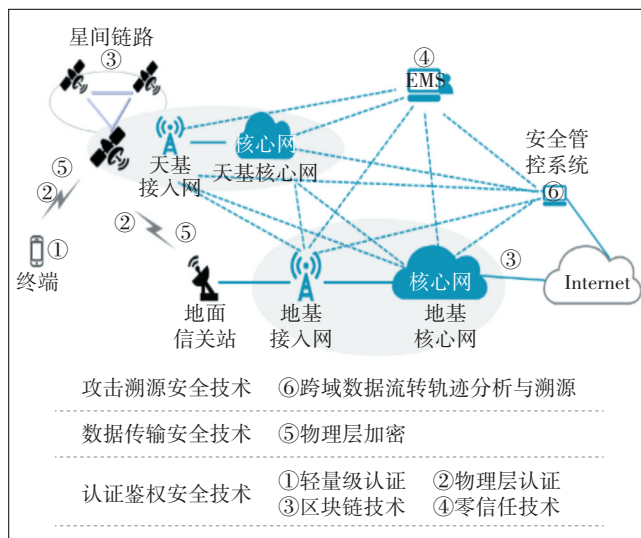


图1 天地一体化网络安全使能技术应用示意

### 4.1 认证鉴权安全技术

#### 4.1.1 轻量级认证

##### 4.1.1.1 安全技术介绍

目前,对于终端的接入认证算法普遍资源开销较大,而天地一体化网络中天基节点资源受限,需要轻量级接入认证技术来支持天地一体化终端安全接入。轻量级认证技术可以利用经典密码机制,优化已有的加密算法结构,或者在不降低安全性能的条件下,减小占用的资源与成本开销,主要实现方式包括设计轻

量级接入认证协议,简化认证流程、压缩协议字段等。

#### 4.1.1.2 天地一体化网络应用场景

天地一体化网络广覆盖场景下,终端接入认证需要满足海量随机接入、低时延、切换频繁等需求,还需要考虑资源受限的天基节点对认证消息的处理能力。在保证安全性的基础上,应用轻量级接入认证技术,既可以满足终端接入认证安全需求,又可以抵御认证拥塞安全风险。

#### 4.1.2 物理层认证

##### 4.1.2.1 安全技术介绍

物理层认证技术通过基于物理层的特征属性来实现对身份和消息的认证,充分利用了底层信号特征属性,具备较高的协议架构兼容性、较高的协议灵活性以及较低的时延等优良特性<sup>[7]</sup>。物理层认证利用无线网络物理层的私有信道特征提供低复杂度、高安全性的安全方案,主要分为如下2种方案。

a) 基于设备指纹的认证。利用硬件设备的电特性差异提取设备独有的特征,将这种唯一标识作为设备的认证指纹。

b) 基于信道指纹的认证。不需要额外的信号提取设备,从无线信道特征入手,利用不同位置设备的信道特征之间存在的互不相关性进行认证。

##### 4.1.2.2 天地一体化网络应用场景

天地一体化网络对比传统地面网络,具有覆盖范围广、受环境影响小、容灾能力强等显著优点,能够提供全球通信、物联网、导航、定位及遥感等多种业务能力,可广泛应用于政治、军事、经济和社会等领域,不同业务场景下也存在不同安全保障能力需求。针对接入认证安全要求高的业务类型,在信道特征明显的场景下,可以考虑采用物理层认证技术,通过丰富和多样化的信号内生特征实现物理层认证,增强接入认证安全性。

#### 4.1.3 区块链技术

##### 4.1.3.1 安全技术介绍

广义来讲,区块链技术是利用链式数据结构存储交易和验证数据,利用密码学算法保证交易数据访问和传输过程中的安全可靠,利用共识机制同步区块链网络和更新数据的一种全新的分布式基础架构。狭义来讲,区块链是一种按照时间顺序,将数据以链式结构进行组织,并以密码学算法保证安全、可追溯且不可篡改的分布式账本<sup>[8]</sup>。区块链为归属权极度分散的分布式网络部署的基础环境,提供了一种面向网络

的信任体系,非常适用于天地一体化网络异构融合分布式部署的网络架构下的认证鉴权。

##### 4.1.3.2 天地一体化网络应用场景

天地一体化网络跨越陆、海、空、天多层级形成融合网络,网络架构前所未有的庞大而复杂,且天基网络、空基网络和地面网络可能由不同的运营实体建设维护,多运营方融合组网场景下存在强烈的多方互信需求。区块链方案是保证多个互联的网络资源可信动态共享的一个较好方案。通过区块链技术进行网元身份管理,可以解决网元身份自主管控、不可篡改、有限匿名、跨域互联多方信任等问题。

#### 4.1.4 零信任技术

##### 4.1.4.1 安全技术介绍

零信任是新一代的网络安全防护理念,它的关键在于“永不信任,持续验证”。零信任是一组围绕资源访问控制的安全策略、技术与过程的统称。零信任默认不信任网络内外的任何人、设备和系统,基于身份认证和授权重新构建访问控制的信任基础,从而确保身份可信、设备可信、应用可信和承载网络可信。零信任是一种以资源保护为核心的网络安全范式,信任必须进行持续评估,确保网络上试图访问的每个设备都通过验证获得信任<sup>[9]</sup>。

##### 4.1.4.2 天地一体化网络应用场景

天地一体化网络拓扑周期性高度动态变化场景下,对验证通信节点、访问身份、承载网络、共享资源的真实性的安全需求进一步提高。网络节点之间的通信应以身份认证为前提,通过启用身份认证流程来保证系统的安全性和独立性。采用零信任接入机制,从对天地一体化用户访问主体的不信任开始,通过持续的身份鉴别和监测评估,动态调整访问策略和权限,实施精细化的访问控制和安全防护,有助于保障天地一体化网络持续、健康、可靠的运行。

表1给出了天地一体化网络认证鉴权安全技术适用场景。

## 4.2 数据传输安全技术

### 4.2.1 物理层加密技术

#### 4.2.1.1 安全技术介绍

传统的提升物理层安全的技术,包括公钥加密和对称加密,存在计算量大和密钥成本管理高的弱点,可能导致高复杂性和高资源消耗,并且无法保证非法窃听者使用暴力算法时不能被破解。物理层加密技术从无线信号传播特点入手,利用无线信道的不可测

表1 天地一体化网络认证鉴权安全技术适用场景

认证对象	认证技术	天地一体化网络应用场景
终端	轻量级认证	天地一体化网络广覆盖场景下,支撑海量低安全需求终端低时延接入
	物理层认证	信道特征明显的场景下,支撑高安全需求终端接入
网元设备、访问身份、承载网络、共享资源	区块链技术	天地一体化融合组网多方信任场景下,满足自主管控、不可篡改及有限匿名需求
	零信任技术	天地一体化网络拓扑周期性高度动态变化场景下,通过持续的身份鉴别和监测评估,保障网络安全

量、不可复制的内生安全属性,将传统需经过终端、接入点和网络之间跨协议层、依靠附加安全字段的加密流程,转化为利用信道指纹和射频指纹在终端与接入点之间通信的物理层实现内生安全。其中,信道指纹和射频指纹蕴藏于信号中,可伴随通信流程一体化完成提取与处理。

#### 4.2.1.2 天地一体化网络应用场景

天地一体化网络覆盖范围更广、通信环境更开放,数据窃听和数据仿冒的安全威胁更加突出,利用物理层加密技术可以有效增强数据传输安全性,实现天地一体化网络中数据传输过程中机密性和完整性保护的安全增强,主要存在以下2个应用场景。

a) 利用无线信道的差异设计与位置强关联的信号传输和处理机制,使得只有在期望位置上的用户才能正确解调信号,而在其他位置上的信号是置乱干扰、污损残缺、不可恢复的。

b) 利用通信双方私有的信道特征,提取无线信道“指纹”特征,提供实时生成、无需分发的快速密钥更新手段,逼近一次一密的完美加密效果。

### 4.3 跨域攻击溯源安全技术

#### 4.3.1 跨域数据流转轨迹分析与溯源

##### 4.3.1.1 安全技术介绍

跨组织、跨地域、复杂多样的网络攻击,为天地一体化网络溯源追踪带来巨大挑战。跨域数据流转轨迹分析和溯源是支撑天地一体化网络安全技术手段建设的重要环节,是信息通报、应急处置的重要技术支撑。跨域数据流转轨迹分析与溯源技术,通过采集天地一体化网络各安全域原始数据信息,结合威胁情报以及业务系统产生的业务管理数据,经数据治理及算法引擎、溯源模型计算后,形成满足数据流转轨迹分析与溯源所需要的场景基础数据,包括攻击者画像、受害者画像、隐藏层画像、攻击路径等信息,最终完成数据流转轨迹路径和溯源分析。

##### 4.3.1.2 天地一体化网络应用场景

天地一体化网络应用数据流转轨迹分析和溯源技术,对空、天、地各域的原始数据进行覆盖全链条的统一采集汇聚,对涉及本网、跨域、跨境任意维度轨迹路径进行流转轨迹分析和溯源,利用大数据分析能力并结合相关的威胁情报信息,对流转轨迹信息进行补充、完善,结合跨域关联分析技术,形成完整的数据流转轨迹路径,最终快速直观地定位运营问题、安全风险、追溯攻击路径和威胁源头。

## 5 总结

天地一体化网络吸收了传统卫星通信和地面移动通信的双重优势,具有广泛的应用场景。但由于天地一体化网络的大时空尺度、动态性强、结构复杂等特点,许多安全问题难以用传统安全理论解决。天地一体化网络安全是全球面临的共同问题,全行业可通过共同的天地一体化网络安全理念,推进天地一体化安全研究,应对潜在的安全挑战,实现天地一体化网络全时全域安全互联。

### 参考文献:

- [1] 3GPP. Study on new radio (NR) to support non-terrestrial networks: TR 38.811 v15.0.0[S/OL]. [2023-05-04]. <ftp://ftp.3gpp.org/Specs/>.
- [2] 3GPP. Solutions for NR to support non-terrestrial networks (NTN): TR 38.821[S/OL]. [2023-05-04]. <ftp://ftp.3gpp.org/Specs/>.
- [3] 缪德山,柴丽,孙建成,等. 5G NTN 关键技术研究及演进展望[J]. 电信科学,2022,38(3):10-21.
- [4] 陈山枝. 关于低轨卫星通信的分析及我国的发展建议[J]. 电信科学,2020,36(6):1-13.
- [5] 陈昊,乔凯,杨欢. 宽带卫星通信系统的安全防护架构研究[J]. 现代导航,2022,13(1):51-56.
- [6] 关汉男,易平,俞敏杰,等. 卫星通信系统安全技术综述[J]. 电信科学,2013,29(7):98-105.
- [7] 任品毅,徐东阳. 无线物理层认证技术:昨天、今天和明天[J]. 中兴通讯技术,2020,26(4):58-66.
- [8] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4):481-494.
- [9] 宋宇飞,周文辉,刘建东,等. 基于零信任的卫星互联网安全防护研究[J]. 天地一体化信息网络,2021,2(3):15-23.

#### 作者简介:

王蕴实,毕业于北京邮电大学,高级工程师,主要从事网络与信息安全研究工作;张曼君,毕业于西安电子科技大学,高级工程师,主要从事网络与信息安全研究工作;徐雷,毕业于北京理工大学,教授级高级工程师,主要从事网络与信息安全研究工作;谢中怀,毕业于香港理工大学,工程师,主要从事网络与信息安全研究工作。