

6G 天地一体化信息网络内生安全技术

季新生^{1,2}, 黄开枝^{1,2}, 邬江兴^{1,2}, 陈亚军¹, 游伟¹

(1. 国家数字交换系统工程技术研究中心, 河南 郑州 450002;

2. 网络通信与安全紫金山实验室, 江苏 南京 211111)

摘要: 6G 天地一体化信息网络面临因网络高度暴露、节点高速运动、计算资源受限等特点带来的安全挑战, 且新架构、新应用、新技术也将引入新的安全问题, 亟须提出普适性安全理论, 一体化解决其功能安全及网络安全问题。为此, 首先阐述网络空间内生安全主要理论基础, 提出 6G 天地一体化信息网络内生安全架构; 然后, 在网络空间内生安全理论的指导下, 从星载系统、6G 地面移动网、星地链路探讨相关安全理论与技术构想; 最后, 从安全认证、高安全通信加密等方面分析天地一体化信息网络通信/安全一体化的认证加密机制, 及传统安全与内生安全技术的交叉融合。

关键词: 6G; 天地一体化信息网络; 网络空间内生安全; DHR 构造; 通信/安全一体化

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2023014

Endogenous Security for the Space-Integrated-Ground Information Network in 6G

Ji Xinsheng^{1,2}, HUANG Kaizhi^{1,2}, WU Jiangxing^{1,2}, CHEN Yajun¹, YOU Wei¹

1. National Digital Switching System Engineering and Technological R&D Center, Zhengzhou 450002, China

2. Purple Mountain Laboratories: Networking, Communications and Security, Nanjing 211111, China

Abstract: The space-integrated-ground information network in 6G is facing security challenges due to its characteristics, such as the high exposure of the network, high-speed movement of nodes, limited computing resources. Moreover, new security issues are certainly introduced in the development of new architectures, new applications, new technologies and so on. It is urgent to propose new universal security theories to overcome safety and security threats by the integrated solutions. For this purpose, this paper first expounded the cyberspace endogenous security and proposed its endogenous security architecture. Then, under the guidance of the cyberspace endogenous security theory, the relevant security theory and practice norms were respectively discussed for onboard systems, 6G ground mobile networks, and satellite-ground links. Finally, the authentication and encryption mechanism of the communication and security integration from the aspects of security authentication and high security communication encryption, and the integration of traditional security technology and endogenous security were analyzed.

Keywords: 6G, space-integrated-ground information network, cyberspace endogenous security, DHR structure, communication and security integration

0 引言

21 世纪以来, 欧美等相继开展了对天地一体化信息网络的研究, 最具代表性的有美军转型卫星通信系统

(Transformational Satellite Communication System, TSAT)^[1]、NASA 空间通信与导航计划 (Space Communications and Navigation, SCaN)^[2]、欧洲全球空间综合通信体系架构 (Integrated Space Infrastructure for Global Communications,

收稿日期: 2023-02-01; 修回日期: 2023-05-04

基金项目: 国家自然科学基金资助项目 (No.U22A2001); 国家重点研发计划资助项目 (No.2020YFB806607, No.2022YFB2902202); 河南省重大科技专项 (No.221100211300)

Foundation Items: The National Natural Science Foundation of China (No.U22A2001), National Key Research&Development Program of China (No.2020YFB806607, No.2022YFB2902202), Major Science and Technology Foundation of Henan Province (No.221100211300)

ISICOM)^[3]以及中国提出的天地一体化信息网络^[4]。

为实现“万物智联、数字孪生”的美好愿景,6G 将深度融合卫星网络、空中通信网等多类异构网络,构建万物智联、高效互通的新型网络,实现空天地一体化的全域无盲区覆盖,随时随地满足“人机物”智能连接需求^[5-6]。

6G 天地一体化信息网络具有卫星节点暴露、信道开放、异构网络互联、拓扑高度动态变化及星上处理能力受限等特点,因而面临诸多安全挑战^[7]。同时,新架构、新应用、新技术也势必引入新安全问题。目前天地一体化信息网络安全主要利用基于密码体制的加密认证机制重点围绕接入认证^[24-30]、安全切换^[31-33]、安全路由^[8]、入侵检测^[9]等方面开展研究,这种“外挂式”安全设计思路不但占用通信和服务资源,降低网络的整体效能^[10],而且无法应对新的甚至未知的安全威胁。

作为未来数字世界、智能社会的关键支撑,6G 天地一体化信息网络需彻底改变传统的“外挂式”“补丁式”网络安全防护机制,充分考虑信息安全需求的同时,深入规划和实现广义功能安全,在安全可信方面实现内生安全^[10-11],从而为未来社会打造坚强可靠的数字化连接底座。为有效解决网络空间普遍存在的内生安全共性问题及其引发的“未知的未知”安全威胁,邬江兴院士提出了网络空间内生安全新理论^[12-15],开辟了网络安全发展新范式,这为 6G 天地一体化信息网络安全提供了有力的科学指导和技术支撑。

1 6G 天地一体化信息网络的安全威胁和需求

6G 天地一体化信息网络组成示意如图 1 所示,包括天基网络、空基网络和地基网络。其中,天基网络主要是高中低轨卫星构建的卫星互联网,空基网络主要将飞机、无人机等临近空间飞行器作为通信平台,地基网络主要包括移动通信网、地面互联网等。

1.1 安全威胁

为实现全时全域无缝立体覆盖,6G 天地一体化信息网络将深度融合天基网络、空基网络与地基网络,形成统一高效的智能网络,不仅网络结构、节点能力发生了根本性变化,而且也带来了巨大的安全挑战,面临卫星互联网传统安全威胁问题^[16-17]。比如:星载设备资源受限,抵御空间复杂环境的安全能力不足;信道完全开放、节点暴露,已被干扰、窃听、仿冒等;海量终端接入、卫星高速运动、节点动态组网,导致接入认证开销大、拓扑变化频繁等问题。

另外,6G 网络架构开放化、网络构件多样化、网络接入泛在化等特点及网络功能虚拟化、边缘化、智能化等新架构或新技术的引入,使得 6G 天地一体化信息网络面临新的安全威胁。网络安全隐患和威胁更加难以确定和控制,未知攻击更加难以防范^[18]。其至少面临 3 类问题:采用“云原生+微服务”架构设计成为 6G 核心网的主要发展趋势,云网深度融合背景下因软硬件漏洞后门带来的网络安全问题^[19];随着网络云化的不断深入,核心网建设处于

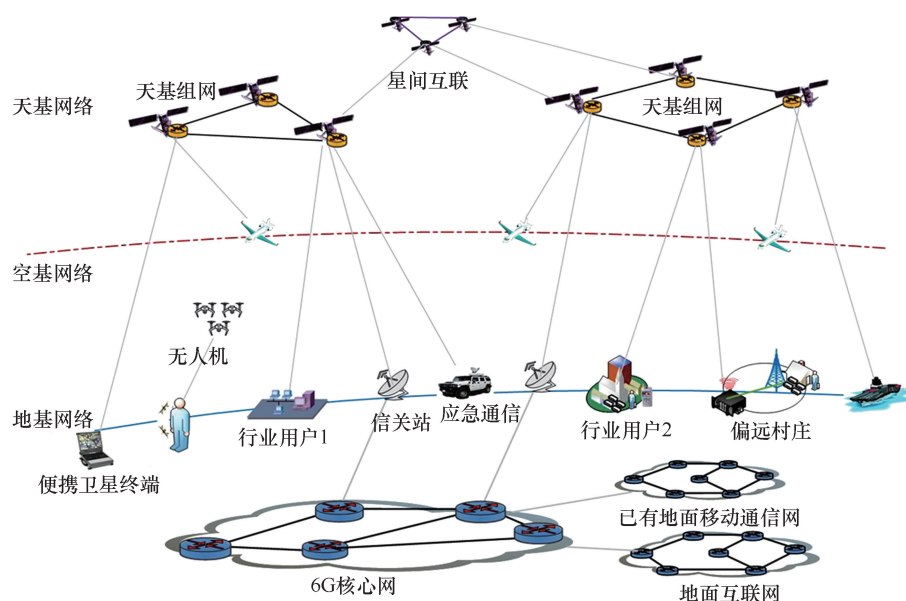


图 1 6G 天地一体化信息网络组成示意

虚拟化到资源池化的优化阶段, NFV 势必得到加快部署, 对核心网的可靠性、稳定性等功能安全带来巨大挑战; 单一 IP 体制难以同时满足物联网、工业互联网、卫星互联网等不同应用场景在性能方面的差异化需求, 将制约 6G 网络的传输性能。

1.2 研究现状

目前, 卫星互联网安全技术方面的研究主要包括抗干扰技术(本文中的安全是指功能安全和信息安全的广义功能安全, 其中抗干扰是功能安全的主要表现形式)、接入认证、安全切换等方面。

卫星网络的干扰方式主要包括压制干扰和欺骗干扰两个方面, 因此抗干扰技术主要围绕上述两个方向开展了抗压制干扰^[20-21]、抗欺骗干扰^[22-23]等研究。近几年, 部分学者利用博弈论数学工具或人工智能等先进技术对卫星抗干扰通信开始探索研究。如参考文献[24]提出一种基于 Stackelberg 博弈和强化学习的最小化路由开销的抗干扰方案。参考文献[25]针对卫星互联网的结构特点和现代通信干扰技术的发展趋势, 探析智能化、网络化抗干扰的基本架构。

在安全接入认证方面, 主要包括基于密钥技术的安全认证、基于区块链技术的安全认证和物理层安全认证等研究方向。基于密钥技术的安全认证主要结合卫星通信系统的节点, 利用传统密钥技术, 如无证书公钥密码体制中公钥加密、私钥签名、公钥验签等技术, 研究身份信息保护^[26]、轻量级^[27]、低时延^[28]的高效认证协议。在基于区块链技术的安全认证方面, 参考文献[29-30]利用区块链不可篡改、去中心化等特点研究了其在低轨卫星通信系统安全认证中的应用。物理层安全认证主要利用多普勒频移这一物理属性检测识别系统信息信号(System Information Signaling, SIS)合法性^[31-32]。针对卫星节点高移动性带来的认证频繁、开销大、效率低等问题, 分别提出了批量用户快速切换认证^[33]、低开销^[34]、轻量级^[35]等高效安全切换认证方法。

综上所述, 目前天地一体化信息网络的主要安全手段沿用了传统打补丁式或附加式的安全技术研发惯性思维, 难以有效应对 6G 天地一体化信息网络新架构、新应用、新技术引入的安全威胁, 特别是无法杜绝基于未知漏洞后门、病毒木马等引发的未知网络攻击。因此, 在 6G 天地一体化信息网络布局之际, 应当立足于安全与通信同步发展的战略需求, 秉承安全与通信一体化设计的技术思路, 在安全理念与架构上进行创新, 催化具有“代际效应”的安全技术, 构建包容、多元、安全和高效的

底座网络生态环境, 在提供高可靠、高可用网络服务的同时提供高可信的安全能力, 从而打造坚强可靠的数字化连接底座。

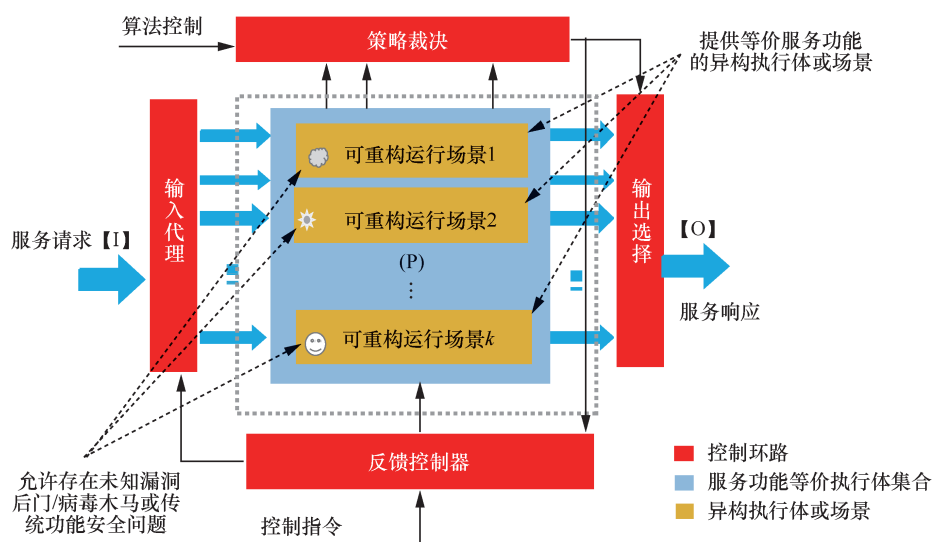
2 网络空间内生安全

邬江兴院士指出信息物理系统的安全问题不仅包括传统类型的随机性或不扰动因素影响(例如随机性错误、失效、故障等可靠性问题, 功能安全问题), 也包括针对目标系统软硬件设计漏洞后门等“暗功能”的未知网络攻击扰动(网络安全问题), 称为广义功能安全问题^[12]。基于外因通过内因起作用、内因起决定性作用的哲学原理, 邬江兴院士创造性地提出网络空间内生安全理论^[12-15], 在不依赖先验知识的条件下, 解决基于目标对象未知内生安全问题的网络攻击问题, 一体化解决功能安全与网络安全交织问题。主要目标是: 发展一种不依赖(但不排斥)漏洞后门发现和攻击特征分析等先验知识的内生安全理论与技术体系, 建立一套有效解决网络空间内生安全共性问题的实践规范, 以创新的“动态异构冗余”(Dynamic Heterogeneity Redundancy, DHR)构造, 提供可量化设计、可验证度量的网络安全与功能安全能力, 有效地防范未知的未知安全威胁。

2.1 DHR 构造

图 2 给出了 DHR 构造的抽象模型^[14], 包含输入代理、功能等价异构执行体或场景集合、策略裁决、输出选择和反馈控制器。输入代理模块根据负反馈控制器的指令将服务请求序列分发到 K 个异构但功能等价的可重构执行场景。策略裁决模块依据系统赋予的参数和算法生成裁决策略, 判定多模输出矢量内容的合规性情况并选择或形成服务响应序列, 一旦发现非期望的裁决状态就会激活负反馈控制环节。负反馈控制模块一旦被激活, 将向导致非期望裁决的异常执行环境发出迁移、替换或在线/离线清洗恢复等操作指令。

这种基于迭代裁决的多维动态重构反馈运行环境, 使得任何独立的人为试错或盲攻击事件都会被异构容错机制所屏蔽, 反馈控制环路会引发异构冗余环境内呈现功能等价条件下的“测不准效应”^[36]。换言之, 由于 DHR 构造固有的随机、多样、冗余特性, 能够产生类似量子物理的测不准效应和生物世界的拟态现象, 使得可以在不依赖(但不排斥)外部先验知识和附加防御措施的情况下, 仅依靠异构配置、策略裁决、反馈控制和多维动态重构等机制, 就能够同时应对“基于暗功能的人为攻击”和软硬件随机性失效引发的故障, 提供功能安全(Safety)和网络安全(Security)一体化的广义功能安全, 从而对抗广义不确定扰动。



注：\$S_k\$间互为异构但具有等价功能\$P\$，\$P=P_1=P_2=\dots=P_k=(P_1 \cup P_2 \cup \dots \cup P_k)\$

图 2 DHR 构造的抽象模型

2.2 DHR 构造内生安全机制

DHR 架构正常运行机制（如图 3 所示）与静态的非相似余度运行环境具有同样的服务功能，以及相同或相似的可靠性与抗攻击性能。但当感知到差模状态时，DHR 架构自动进入差模事件运行机制（如图 4 所示），当前运行环境内动态迭代与收敛机制被激活，直到策略裁决部件重新回到设计想定的正常运行机制。不论何种原因，DHR 架构一旦感知到当前运行环境内存在差模输出状态，反馈控制机制就试图策略性地调度当前执行体集合中的元素，或对问题执行体本身做清洗恢复等改变运行状态的操作，或激活功能等价条件下的多维动态重构机制，自动选择合适的执行体元素（或场景）以消除非期望的裁决差异。因

而，DHR 架构从机理上就具备广义功能安全属性。

基于 DHR 架构的内生安全（广义功能安全）技术能将“未知的未知安全威胁”变换为“已知的未知安全问题”，理论上可以 100%地抑制 DHR 构造内以差模形态呈现的广义不确定扰动，并能将构造内共模形态的广义不确定扰动的逃逸概率控制在设定阈值内。这就为网络空间安全防御的有效性提供了可量化设计、可验证度量的新发展范式^[12]。

3 6G 天地一体化信息网络内生安全架构

网络空间内生安全理论开辟了防御“未知的未知”安全威胁的网络空间安全新范式，利用 DHR 架构构造内生安

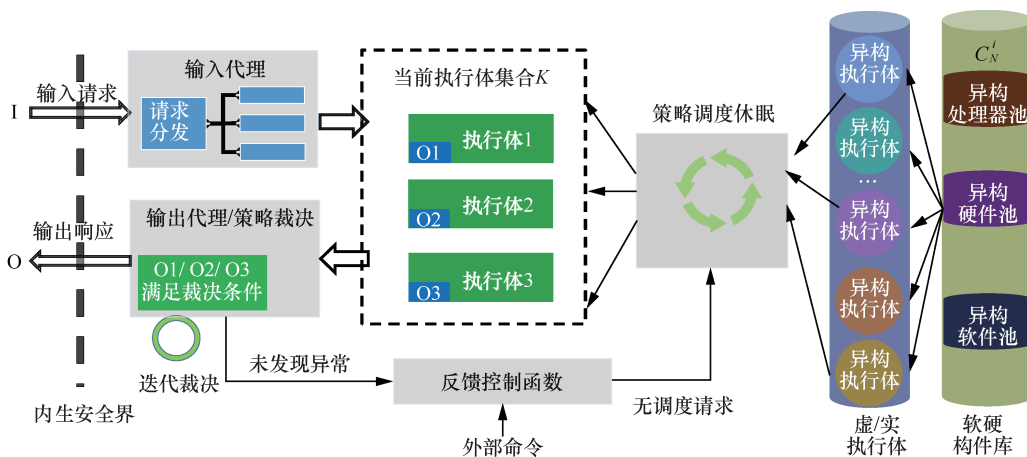


图 3 DHR 架构正常运行机制

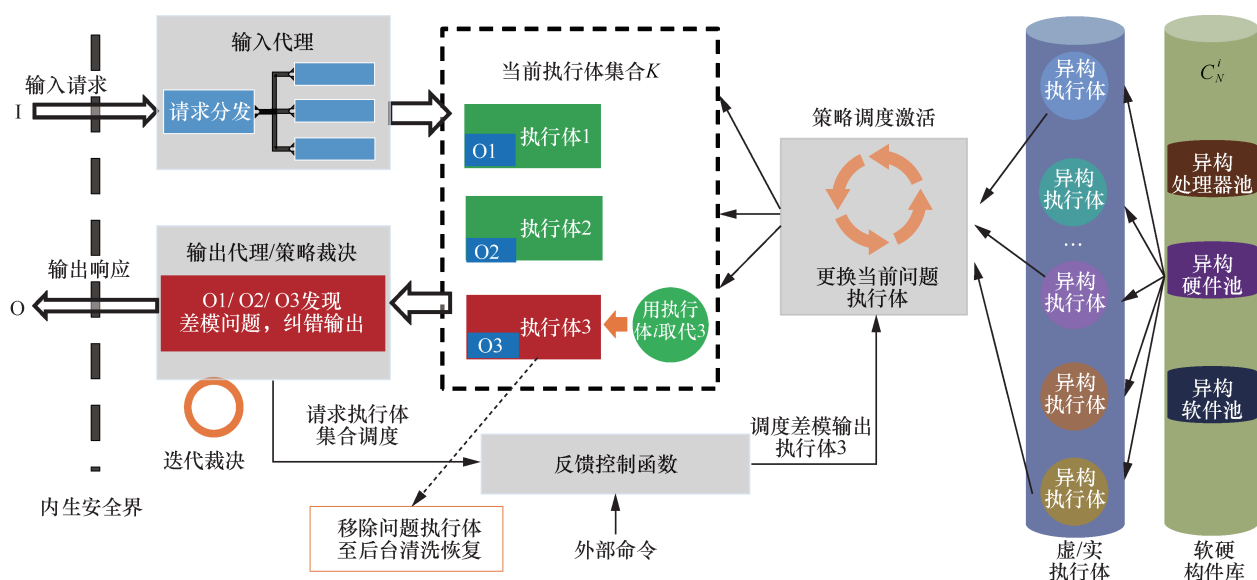


图4 DHR 架构差模事件运行机制

全功能,形成抵御已知和未知威胁的内生安全效应,不仅能够增强高可靠、高可用、高可信三位一体的广义鲁棒服务性能,同时也带来内生的、普适性的网络弹性功能。这将成为有效解决网络安全问题的重要途径。在网络空间内生安全理论的指导下,针对6G天地一体化信息网络架构的特点,整体考虑6G天地一体化信息网络底层网络与上层应用服务的安全保障,开辟通信与安全一体化的内生安全新路径,探索从广义功能安全与通信服务共有的本源属性出发的内生安全机制,打破技术性能裸奔和安全措施补丁的传统思维,构建革新性的具有内生安全属性

的网络安全架构,打造具有内生安全基因的弹性天地一体化信息网络。

6G 天地一体化信息网络应该是弹性的、网络安全的、保护隐私的、功能安全的、可靠的,须将广义功能安全(包括安全性、适应性、自主性和可靠性等)作为网络架构的最底层,建立内生安全模型,设计6G天地一体化信息网络内生安全架构。如图5所示,具体表现在以下几个方面:针对星载核心设备资源受限等特点,研究基于结构内生的安全可靠一体化技术,在抵抗空间恶劣环境的同时,提供不依赖攻击规则的安全防护能力;

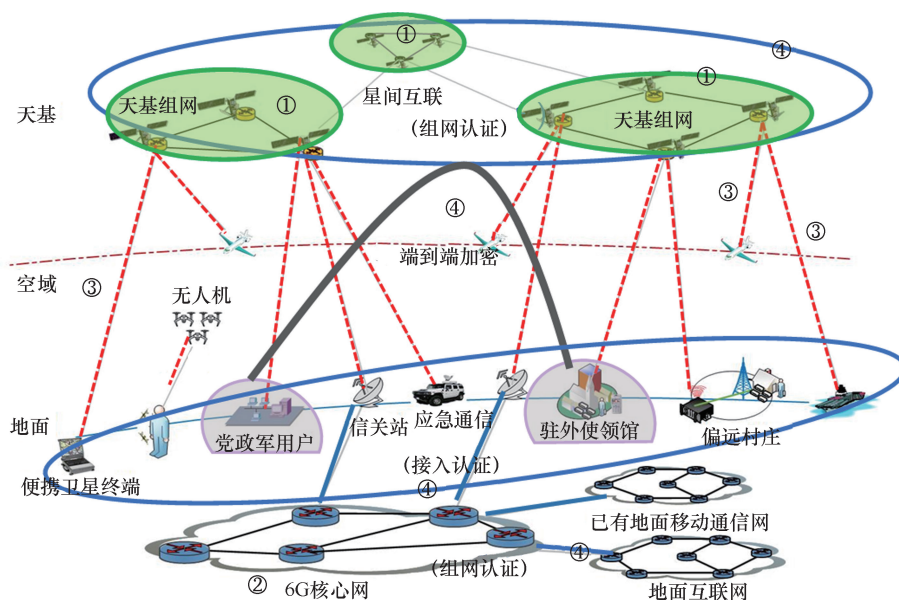


图5 6G 天地一体化信息网络内生安全架构

针对 6G 地面移动网内生性缺陷产生的内生安全问题, 研究 6G 内生安全技术, 有效应对漏洞后门带来的未知网络攻击; 针对星地链路信道开放性带来的安全短板问题, 研究 RIS 赋能的星地链路无线内生安全, 解决用户链路和无线密钥推送的安全最短板; 针对节点动态组网、海量终端接入、高安全等级通信等需求, 研究通信/安全一体的认证加密机制, 构建传统安全与内生安全高效融合体系。

4 星载系统内生安全

目前, 已有通过商业级器件的冗余实现了宇航级器件的效果, 代表了星载核心功能设计趋势, 未来卫星将具备构建冗余执行体的资源条件, 基于动态异构冗余架构设计星上核心功能, 实现结构内生的安全可靠一体化, 在实现可靠性的同时提升安全性, 赋予卫星抵御未知安全攻击的能力。

但是, 星上执行体资源有限, 恶劣空间环境及人为攻击造成的执行体扰动会影响系统的可靠性保障与安全防护。因此星上设计时, 在计算存储资源受限的条件下, 为解决单一架构导致的漏洞利用和被后门的问题, 要设计卫星核心功能异构多样化软硬件环境构建、异构执行体选择及相异性方法, 精准化构建功能等价、结构不同的执行体, 做到“隘口防御”。针对空间苛刻的环境, 例如粒子辐射、高低温等易造成执行体随机扰动, 进而影响攻击判决的问题, 建立资源、成本、可靠、安全的优化模型, 适当引入同构资源, 对执行体合理编配调度, 实现同构、异构执行体的效能协同, 做到可靠性、安全性、稳定性、经济性的统一, 实现综合防御效果的最优化和代价的最小化。

5 6G 地面移动网内生安全

卫星通信安全架构基本沿用地面移动通信网络架构, 关键安全防护设施部署在地面关口。因此, 6G 地面移动网络安全架构将是 6G 天地一体化信息网络的重要组成部分。6G 地面移动网内生安全系统包括 6G 内生安全云原生平台和 6G 内生安全微服务两部分, 内生安全云原生平台作为 6G 天地一体化信息网络地面移动网内生安全的基础环境, 为其提供云计算与内生安全的基础平台能力; 内生安全微服务则承载在云原生底座上, 提供控制面、用户面、数据面、智能面、安全面等功能。

5.1 6G 内生安全云原生平台

6G 内生安全云原生平台遵循功能、安全一体化设计的理念, 将内生安全功能融入 6G 云原生平台, 使其成为

云原生平台的一项基础能力。

6G 内生安全云原生平台架构可分为基础设施层、云平台层和应用层。在基础设施层, 传统云平台一般对底层计算、存储和网络等资源进行统一管理, 形成云计算集群。而在内生安全云原生平台中, 不仅能统一纳管多个异构计算、存储和网络资源, 并形成多个异构集群, 而且还能对输入代理、裁决器等拟态括号进行抽象并统一管理, 形成拟态括号资源池, 实现内生安全资源的灵活分配与弹性调度。基于基础设施层, 内生安全云原生平台以容器云编排管理框架 Kubernetes 为核心, 集成内生安全模块, 例如异构镜像仓库、异构运行时和多样化编译流水线等模块, 为上层应用提供内生安全能力的基础支撑。其中, 多样化编译流水线通过对云原生 DevOps 进行改造, 将多样化编译技术集成到持续集成 (Continuous Integration, CI) /持续部署 (Continuous Deployment, CD) 流水线中, 为拟态执行体的异构性提供支撑。在多样化编译流水线中, 通过对同一份源代码使用不同的编译策略, 提高应用层的异构度; 通过使用不同的基础环境打包容器镜像, 提高执行体镜像的异构度。基于多样化编译流水线, 应用通过一份源代码即可自动化产生大量异构的镜像, 为应用拟态化提供了异构能力基础。

在云平台层, 通过对微服务拟态化共性需求进行提炼, 形成内生安全微服务框架。内生安全微服务框架基于 Kubernetes 的应用管理的控制器模式, 融合拟态防御的动态异构冗余 (DHR) 架构, 提供了一种云原生的拟态应用管理功能。用户可以通过调用 Kubernetes 的 API 入口, 实现拟态应用的细粒度控制与管理功能。尤其是针对云原生下的微服务化应用, 用户可以通过配置的方式灵活选择需要使用拟态技术防护的微服务, 实现内生安全能力的灵活分配与管理。

5.2 6G 内生安全微服务

6G 地面移动网络将采用全服务化架构, 服务化功能层中的控制面、用户面、数据面、智能面、安全面等各个面之间, 以及每一面内部的各个网络功能都统一在服务化架构下, 采用模块化、服务化设计, 利用统一的服务框架技术进行服务的自组织, 并通过服务化接口彼此交互。全服务化架构是服务化架构的进一步深化, 在服务框架、服务接口、原子服务等方面做了增强, 以适应网络的分布式组织、服务的智能化调度、行业专网的灵活化部署。

服务化设计遵循“高内聚”“松耦合”原则, 每个服务功能由一组职责单一的微服务共同构成。针对微服务通信故障或微服务功能设计上的漏洞后门带来的未知安全

威胁,可利用 DHR 架构进行内生安全微服务构造。拟态构造微服务的难点在于:难点一,微服务数量众多,导致内生安全的微服务功能链过于冗长和繁杂;难点二,微服务接口众多,拟态裁决器需要满足不同微服务消息的裁决;难点三,大量微服务消息被汇聚和分发,拟态控制器需要满足高可用。针对难点一,内生安全微服务框架需提供灵活编排微服务内生安全的能力,即满足用户以配置的方式灵活选择需要使用拟态技术防护的微服务。针对难点二,通过提炼微服务通信的共性特征,设计实现面向微服务化的通用拟态裁决器,以数据驱动的方式完成异构微服务之间的输出裁决,对于新上线的微服务,无须对裁决器进行重新适配。针对难点三,内生安全微服务框架采用分布式架构,控制器可以分布在不同的分布式网络中,网络具备自组织、自管理、自优化的能力,通过框架之间的协同来支持其高可靠、高并发和低时延。

内生安全微服务框架能自动化地为微服务应用提供拟态基础能力,包括拟态架构编排、异构执行体的选择、定时执行体轮换机制、受攻击执行体轮换机制等。具体来说,内生安全微服务框架能够根据微服务化应用中微服务之间的调用关系以及所需防护的微服务,自动化生成具有 DHR 架构的拟态微服务化应用。当创建多个异构的执行体时,会考虑底层计算节点、容器运行时、镜像等多个层次的异构属性,选择异构度最大的方案创建执行体。在拟态应用的运行过程中,拟态控制模块会定时对执行体副本进行轮换,以迷惑攻击者。同时,当拟态裁决器感知到有执行体受攻击时,也会通知拟态控制模块,从而对受攻击的执行体进行清洗与轮换。通过上述功能,内生安全微服务框架能够对拟态应用的全生命周期进行管理,为应用赋予内生安全能力。

6 星地链路无线内生安全

电磁波传播开放性这一内源性缺陷是造成星地无线链路安全问题的根源,包括主动攻击、被动窃听等信息安全问题,以及由自然扰动造成的随机衰落和人为扰动造成的有意无意干扰等功能安全问题。要从根本上解决星地链路因电磁传播开放性造成的无线内生安全问题,只能依靠内生安全手段。无线内生安全技术^[37-39]基于无线接入电磁波传播机理,从安全与通信的共生属性入手,挖掘无线信道各点异性、动态时变的天然内生属性,设计安全与通信一体化的安全机制,打破了外挂密码认证技术的“打补丁式”技术路线。这为 6G 天地一体化信息网络星地链路安全设计提供了新的技术思路。

6.1 星地链路无线内生安全 DHR 构造

典型无线通信系统可以看作一种天然结合人工的 DHR 构造,具有 DHR 构造的天然内生属性^[37-39]。6G 天地一体化信息网络星地链路无线内生安全 DHR 架构模型如图 6 所示,星地无线链路、发信机和接收机分别对应 DHR 的异构执行体或场景、输入代理和输出选择。星地无线链路作为 DHR 异构执行体或场景,如何改造并定制无线环境,使异构执行体(即差异化星地链路)的构造成成为 DHR 构造的关键。要改造并定制星地链路无线环境必须基于内生属性实现内生构造,塑造对抗无线扰动的最优无线链路环境。具体表现在以下几个方面:通过对星地无线链路进行动态编程和按需重构对抗自然扰动;通过塑造、拉大星地无线链路的差异性对抗人为扰动;通过改造强化星地无线链路的内生安全属性对抗无线安全威胁。这为星地链路无线内生安全的实现与落地提供了理论指导。

6.2 RIS 赋能的星地链路无线内生安全构想

卫星通信由于星上资源受限、关键节点(卫星)暴露

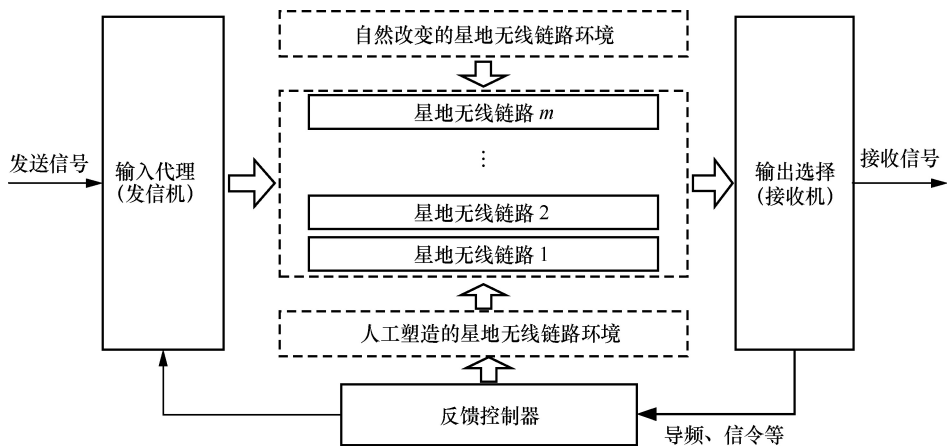


图 6 6G 天地一体化信息网络星地链路无线内生安全 DHR 架构模型

等问题, 现有安全防护能力存在“天弱地强”的现实困境^[40]。利用信道特征内生安全属性生成的内生安全密钥能够在网络边缘实现认证和加密, 不但避免了开放环境中推送密钥导致密钥泄露的问题, 而且有效降低了链路资源消耗, 这为天地一体化信息网络安全补强短板、弥合差距提供了有效的技术途径^[41-43]。但由于单一星地链路散射路径有限, 因此同一波束覆盖范围内信道随机性弱、差异性小, 空域、时域的自由度受限, 利用星地链路信道生成内生安全密钥的速率十分有限。

智能超表面 (Reconfigurable Intelligent Surface, RIS) 能够通过 FPGA 实时控制改变每个粒子单元的状态^[44-45], 进而控制电磁波传播方向、相位、幅度、频率和极化等特性, 实现对无线环境的实时重构、动态编程。基于 RIS 的柔性可重构和操控电磁波的特性, 可构造阵元具有时空二维敏捷可重构特性的 DHR 阵列。该阵列具有以下特性: 同一时刻, 不同的阵元具有异构的方向图; 不同时刻, 同一阵元也具有异构的方向图。因此, DHR 阵列的天线阵元通过动态捷变与异构构造, 在利用自然无线环境和挖掘内生安全属性的同时, 通过“塑造定制”无线环境, 主动改造内生安全属性, 为实现可控的异构执行体构造提供了技术途径。

RIS 赋能的星地链路无线内生安全方案构想如图 7 所示, 遵照“构造决定论”的设计理念, 结合基于 RIS 的 DHR 阵列构造技术和无线内生安全技术, 通过人工塑造星地链路无线环境, 主动构造无线内生安全属性, 在物理层实现对抗无线广义不确定扰动的星地通信广义鲁棒控制^[46], 同时实现功能安全和信息安全一体化设计。具体表现为: 利用空域和时域提供的自由度, 拉大星地无线链路差异性, 在提高通信容量的同时提升波束方向的分辨率和内生安全密钥生成速率; 利用动态捷变改造星地无线链路的随机性和时变性基因, 利用异构改造不同信道的相关性和差异性基因, 提升信道指纹安全能力。因此, 利用基于 RIS 的 DHR 阵列的动态捷变特性, 通过人工操控电磁星地无线链路和改造定制无线内生安全属性, 能够显著提升星地链路信道的随机性, 明显拉大信道差异性, 在提高通信容量的同时有效提升波束方向的分辨率和解决内生密钥生成速率不足的问题, 为 6G 天地一体化信息网络星地链路提供安全增量。具体地, 针对星地链路内生密钥生成能力受限问题, 利用 RIS 的捷变特性和可重构特性调控并定制星地链路无线环境, 如在星上系统部署 RIS 在空时二维快速调控发射波束, 从根本上提高无线环境的随机性和时变性。同时, 通信双方叠加利用多星协作、拓扑时变、

空间摄动等产生的无线信道随机动态变化特性, 产生内生安全密钥, 用于数据加密、身份认证, 能够有效应对因星地链路电磁传播开放性这一内源性缺陷带来的安全威胁。

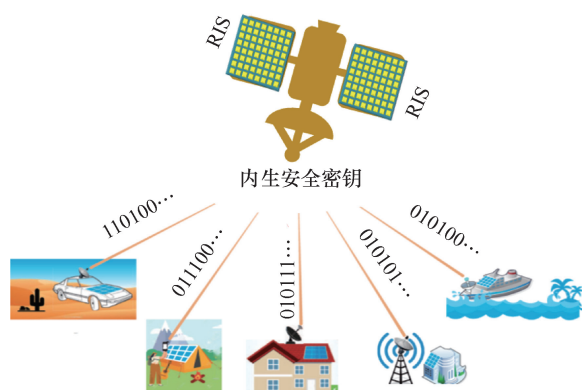


图 7 RIS 赋能的星地链路无线内生安全构想

7 通信/安全一体的认证加密机制

针对 6G 天地一体化信息网络明确的安全需求和已知的安全威胁, 可以继承和发展卫星互联网安全技术, 在计算安全理论框架下开展传统密码体系的认证、加密等安全技术的增强研究, 进行点防御, 实现“特异性免疫”。另外, 在内生安全理论框架下开展内生安全构造研究, 实施面防御, 实现“非特异性免疫”。通过内生安全与传统安全技术的融合形成“点面融合”的防御体系, 不仅能在未知安全威胁的环境中实现安全, 还能针对确定安全威胁进行高效精准的“杀毒灭菌”^[35], 达到“1+1>2”的效果。下面分别就 6G 天地一体化信息网络安全认证、高安全加密两个方面阐述通信/安全一体的认证加密机制, 分析内生安全与传统安全融合机理。

7.1 6G 天地一体化信息网络安全认证

6G 天地一体化信息网络支持卫星节点、地面节点、空中节点等海量节点的接入认证, 且卫星节点始终处于高速运转状态, 需要频繁地进出网络, 导致网络拓扑时刻发生变化。因此, 结合 6G 天地一体化信息网络特点, 通过融合传统安全与内生安全技术、优化传统认证机制设计高效接入认证机制是重点研究方向, 具体如下。

一是与通信流程一体化设计的组网认证机制。采用星间/星地/地地认证与通信流程一体化融合设计的思想, 研究星地网络拓扑结构高速动态变化下的内嵌互联认证方法, 通过重构内嵌、参数可变压缩等技术, 实现通信认证紧耦、安全不可绕过、协议开销可控的网络实体可信与组网认证。

二是资源受限下的海量终端接入认证。研究轻量化的终端接入认证与安全切换技术, 包括基于终端低功耗聚合

签名的群组式认证的方式、面向低轨卫星频繁切换下的基于轨迹预测的信任高效传递,实现终端安全快速可信接入、切换保持和持续服务。

三是星地跨层异构认证协议融合机制。研究 6G 天线一体化网络多种接入机制下的跨层融合认证与信任传递,包括射频/信道/智能卡/口令等多认证体制策略控制、内生信道指纹与多元身份融合关联、轻量级物理层辅助认证与跨层信任传递等技术,实现异构认证体制的融合互信。

7.2 6G 天地一体化信息网络高安全通信加密

依托 6G 天地一体化信息网络,采用高等级加密防护体制,为行业用户建立高安全等级专网,高安全等级加密机制研究主要如下。

一是跨域联合密码管理机制。6G 卫星网络可为各种用户提供全域通信保障,需支持不同业务的加密传输。面向不同安全等级、加密算法、网络体制、应用类型,研究密码管理及切换机制,设计密码资源按级、域和任务的自动化管理方法。

二是高效密钥协商与更新。针对网络拓扑动态变化、链路间歇中断以及单星过顶时间短等特点,研究轻量化的签密方案,设计交互次数少、运算效率高的交互式密钥协商机制,提高密钥协商的效率。

三是高安全轻量化密码管理协议。在线密码管理对于信道带宽及传输时延均有一定的要求,针对卫星信道带宽受限、传输距离远的特点,以及传统基于 TCP/IP 密码管理协议适应性不够,开展轻量化密码管理协议的研究,减少协议开销及占用的信道资源,并适应卫星信道长时延的特点;同时,针对标准的密码协议进行适应性改进,以提升其安全性。

8 结束语

本文围绕 6G 天地一体化信息网络高可信、高可靠、高可用、高可控、高保密、高隐私等需求,以网络空间内生安全理论为指导,探索了 6G 天地一体化信息网络内生安全基础理论和关键技术。针对 6G 天地一体化信息网络的星载系统、6G 地面移动网、星地链路分别提出了相应的内生安全构想,同时也总结了内生安全与传统安全的融合发展需求,期望为 6G 天地一体化信息网络实现技术性能与安全可控一体化发展提供参考。

参考文献

[1] 刘铁锋,张明华. 美军转型卫星通信系统及其发展[J]. 卫星与网络, 2011(5): 62-63.

LIU T F, ZHANG M H. The transformation satellite communication system of US army and its development[J]. Satellite & Network, 2011(5): 62-63.

[2] 颜洁,彭玉婷. NASA 空间通信与导航网络现状及未来发展[J]. 国际太空, 2018(7): 25-31.

YAN J, PENG Y T. Current status and future development of NASA space communications and navigation (SCaN) network[J]. Space International, 2018(7): 25-31.

[3] 梁俊,胡猛,管桦,等. 空间骨干网络体系架构与关键技术研究[J]. 空军工程大学学报(自然科学版), 2016, 17(4): 52-58.

LIANG J, HU M, GUAN H, et al. Research on space backbone network architecture and key technologies[J]. Journal of Air Force Engineering University (Natural Science Edition), 2016, 17(4): 52-58.

[4] 汪春霆,翟立君,徐晓帆. 天地一体化信息网络发展与展望[J]. 无线电通信技术, 2020, 46(5): 491-504.

WANG C T, ZHAI L J, XU X F. Development and prospects of space-terrestrial integrated information network[J]. Radio Communications Technology, 2020, 46(5): 491-504.

[5] LI R. 5th ITU-T workshop on network 2030 concluding remarks[EB]. 2019.

[6] 吴晓文,焦侦丰,凌翔,等. 面向 6G 的卫星通信网络架构展望[J]. 电信科学, 2021, 37(7): 1-14.

WU X W, JIAO Z F, LING X, et al. Outlook on satellite communications network architecture for 6G[J]. Telecommunications Science, 2021, 37(7): 1-14.

[7] 李风华,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.

[8] CAO S, DANG S, ZHANG Y, et al. A blockchain-based access control and intrusion detection framework for satellite communication systems[J]. Computer Communications, 2021, 172: 216-225.

[9] ZHAN Y F, ZENG G M, PAN X H. Networked TT&C for mega satellite constellations: a security perspective[J]. China Communications, 2022, 19(9): 58-76.

[10] 徐晖,孙韶辉. 面向 6G 的天地一体化信息网络架构研究[J]. 天地一体化信息网络, 2021, 2(4): 1-9.

XU H, SUN S H. Research on network architecture for the space-integrated-ground information network in 6G[J]. Space-Integrated-Ground Information Networks, 2021, 2(4): 1-9.

[11] IMT-2030 (6G) 推进组. 6G 前沿关键技术研究[R]. 2022.

IMT-2030 (6G) Promotion Group. Frontier key technologies for 6G mobile communications[R]. 2022.

[12] 邬江兴. 网络空间内生安全发展范式[J]. 中国科学(信息科学),

- 2022, 52(2): 189-204.
- WU J X. Development paradigms of cyberspace endogenous safety and security[J]. *Scientia Sinica(Informationis)*, 2022, 52(2): 189-204.
- [13] 邬江兴. 网络空间拟态防御导论-上册[M]. 北京: 科学出版社, 2017.
- WU J X. Introduction to cyberspace mimic defense[M]. Beijing: Science Press, 2017.
- [14] 邬江兴. 网络空间拟态防御原理-下册: 广义鲁棒控制与内生安全[M]. 北京: 科学出版社, 2018.
- WU J X. Principle of cyberspace mimic defense-generalized robust control and endogenous security[M]. Beijing: Science Press, 2018.
- [15] 邬江兴. 网络空间内生安全-下册: 拟态防御与广义鲁棒控制[M]. 北京: 科学出版社, 2020.
- WU J X. Cyberspace endogenous safety and security-mimic defense and generalized robust control[M]. Beijing: Science Press, 2020.
- [16] AHMAD I, SUOMALAINEN J, PORAMBAGE P, et al. Security of satellite-terrestrial communications: challenges and potential solutions[J]. *IEEE Access*, 2022, 10: 96038-96052.
- [17] HAN S, LI J X, MENG W X, et al. Challenges of physical layer security in a satellite-terrestrial network[J]. *IEEE Network*, 2022, 36(3): 98-104.
- [18] 中国移动研究院. 2030+愿景与需求报告[R]. 2020.
- Research Institute of China Mobile Communication Co., Ltd. 2030 + vision and requirements report[R]. 2020.
- [19] Yushan Synopsys. 2020 open source security and risk analysis (OSSRA) report[R]. 2020.
- [20] FAN Y W, ZHANG Z H, TRINKLE M, et al. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids[J]. *IEEE Transactions on Smart Grid*, 2014, 6(6): 2659-2668.
- [21] YU J H, GONG Y, FANG J H, et al. Let us work together: cooperative beamforming for UAV anti-jamming in space-air-ground networks[J]. *IEEE Internet of Things Journal*, 2022, 9(17): 15607-15617.
- [22] DAI L W, RIZOS C, WANG J L. The role of pseudo-satellite signals in precise GPS-based positioning[J]. *Journal of Geospatial Engineering*, 2001, 3(1): 33-44.
- [23] LI J Z, ZHU X W, OUYANG M J, et al. GNSS spoofing jamming detection based on generative adversarial network[J]. *IEEE Sensors Journal*, 2021, 21(20): 22823-22832.
- [24] HAN C, HUO L Y, TONG X H, et al. Spatial anti-jamming scheme for Internet of satellites based on the deep reinforcement learning and stackelberg game[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(5): 5331-5342.
- [25] 韩晨, 刘爱军, 安康. 卫星互联网抗干扰策略研究展望[J]. *天地一体化信息网络*, 2022(1): 50-55.
- HAN C, LIU A J, AN K. Research prospect of anti-jamming strategy for the satellite Internet[J]. *Space-Integrated-Ground Information Networks*, 2022(1): 50-55.
- [26] 苗婷婷, 刘笑凯, 姬胜凯, 等. 基于 CL-PKC 的卫星通信认证技术研究[J]. *信息技术与网络安全*, 2022, 41(6): 18-21.
- MIAO T T, LIU X K, JI S K, et al. Research on satellite communication authentication technology based on CL-PKC[J]. *Information Technology and Network Security*, 2022, 41(6): 18-21.
- [27] LI K, CUI Q M, ZHU Z B, et al. Lightweight, privacy-preserving handover authentication for integrated terrestrial-satellite networks[C]//*Proceedings of ICC 2022-IEEE International Conference on Communications*. Piscataway: IEEE Press, 2022: 25-31.
- [28] LIU Y, NI L Q, PENG M G. A secure and efficient authentication protocol for satellite-terrestrial networks[J]. *IEEE Internet of Things Journal*, 2023, 10(7): 5810-5822.
- [29] WANG B Y, CHANG Z, LI S C, et al. An efficient and privacy-preserving blockchain-based authentication scheme for low earth orbit satellite-assisted Internet of Things[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2022, 58(6): 5153-5164.
- [30] XIONG T, LIU J, ZHANG R, et al. Delay-aware cooperative caching for on-chain authentication in LEO satellite communication systems[C]//*Proceedings of ICC 2022 - IEEE International Conference on Communications*. Piscataway: IEEE Press, 2022: 3058-3063.
- [31] FU Q Y, FENG Y H, WANG H M, et al. Initial satellite access authentication based on Doppler frequency shift[J]. *IEEE Wireless Communications Letters*, 2021, 10(3): 498-502.
- [32] TOPAL O A, KARABULUT K G. Physical layer authentication for LEO satellite constellations[C]//*Proceedings of 2022 IEEE Wireless Communications and Networking Conference (WCNC)*. Piscataway: IEEE Press, 2022: 1952-1957.
- [33] 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.
- [34] 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.
- [35] 黎海燕, 王利明, 徐震, 等. LEO 卫星网络中星间切换的安全机制研究[J]. *智能计算机与应用*, 2018, 8(2): 7-13.
- LI H Y, WANG L M, XU Z, et al. Research on security mechanism of inter-satellite handover in LEO satellite scenario[J]. *Intelligent Computer and Applications*, 2018, 8(2): 7-13.
- [36] LIU L S, YU M L, YAN Z. A concise course on advanced quantum mechanics[M]. Beijing: Science Press, 2009.
- [37] JIN L, HU X Y, LOU Y M, et al. Introduction to wireless endogen-

- ous security and safety: problems, attributes, structures and functions[J]. China Communications, 2021, 18(9): 88-99.
- [38] 金梁, 楼洋明, 孙小丽, 等. 6G 无线内生安全理念与构想[J]. 中国科学(信息科学), 2023, 53(2): 344-364.
- JIN L, LOU Y M, SUN X L, et al. Concept and vision of 6G wireless endogenous safety and security[J]. Scientia Sinica (Information), 2023, 53(2): 344-364.
- [39] JI X S, WU J X, JIN L, et al. Discussion on a new paradigm of endogenous security towards 6G networks[J]. Frontiers of Information Technology & Electronic Engineering, 2022, 23(10): 1421-1450.
- [40] 吴巍, 秦鹏, 冯旭, 等. 关于天地一体化信息网络发展建设的思考[J]. 电信科学, 2017, 33(12): 3-9.
- WU W, QIN P, FENG X, et al. Reflections on the development and construction of space-ground integration information network[J]. Telecommunications Science, 2017, 33(12): 3-9.
- [41] 张杰, 熊俊, 马东堂. 多波束卫星通信系统中的物理层安全传输算法[J]. 电子技术应用, 2014, 40(11): 116-119.
- ZHANG J, XIONG J, MA D T. The physical layer security transmission algorithms in multi-beam satellite communication system[J]. Application of Electronic Technique, 2014, 40(11): 116-119.
- [42] YIN Z S, JIA M, CHENG N, et al. UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(3): 2739-2751.
- [43] ENDO H, SASAKI M. Secret key agreement for satellite laser communications. Advances in communications satellite systems[C]//37th International Communications Satellite Systems Conference (ICSSC-2019), Piscataway: IEEE Press, 2019: 1-11.
- [44] LIANG Y C, CHEN J, LONG R Z, et al. Reconfigurable intelligent surfaces for smart wireless environments: channel estimation, system design and applications in 6G networks[J]. Science China Information Sciences, 2021, 64(10): 1-21.
- [45] IMT-2030 (6G) 推进组. 智能超表面研究报告[R]. 2022.
- IMT-2030 (6G) Promotion Group. Research on reconfigurable intelligent surface[R]. 2022.
- [46] ZHENG B X, LIN S E, ZHANG R. Intelligent reflecting surface-aided LEO satellite communication: cooperative passive beamforming and distributed channel estimation[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(10): 3057-3070.

[作者简介]



季新生 (1968—), 男, 硕士, 国家数字交换系统工程技术研究中心总工程师, 国家 6G 总体技术组专家, 无线通信协同创新中心无线安全方向首席科学家, 移动互联网安全技术工程研究中心副主任, 国家自然科学基金创新研究群体学术带头人。曾获国家科技进步奖一等奖 3 项、国家科技进步奖创新团队奖。主要研究方向为下一代移动通信和网络空间安全。



黄开枝 (1973—), 女, 博士, 国家数字交换系统工程技术研究中心教授, 新一代宽带无线移动通信网重大科技专项核心专家库专家, 国家重点研发计划和国家自然科学基金项目评审专家。曾获国家科技进步奖创新团队奖。主要研究方向为无线网络安全和信号处理。



邬江兴 (1953—), 男, 中国工程院院士, 国家数字交换系统工程技术研究中心主任、教授, 曾任国家 863 计划通信技术主题专家组副组长, 863 计划信息领域专家组副组长, 国家移动通信重大专项 (第 3 专项) 论证委员会主任, 国家 NGB 专家委员会主任兼总工程师, 国家三网融合专家组副组长, “十三五”国家重大科技专项工程——天地一体化信息网络专家组副组长。曾获国家科技进步一等奖 3 项、二等奖 4 项, 国家科技进步奖创新团队奖。主要研究方向为网络空间安全和网络架构。



陈亚军 (1988—), 男, 博士, 国家数字交换系统工程技术研究中心助理研究员, 主要研究方向为无线网络安全。



游伟 (1984—), 男, 博士, 国家数字交换系统工程技术研究中心副教授, 主要研究方向为移动通信网络体系架构、移动通信网安全。