



## 编者按

虽然目前全球 5G 网络仍处于蓬勃商用的早期阶段,但面向 2030 年之后的未来网络需求,全球 6G 的科研竞赛已经拉开帷幕.值得特别关注的是,在当前世界各国关于 6G 愿景、需求和关键技术的初期探讨中,安全受到了异乎寻常的重视.

首先,中国政府和研究机构在国际上率先提出内生安全 6G 的愿景.一方面,面向 6G 将为人机物高度融合的世界提供关键服务的核心需求,对移动通信网络安全内涵和外延做出新的拓展,要求 6G 安全在传统信息安全机密性、完整性、可用性和隐私保护基础之上,还需重视 6G 网络的广义鲁棒控制和广义功能安全.另一方面,面向 6G 需在高强度复杂网络条件下具备使命确保的保底需求,必须打破技术性能裸奔和安全措施后补的传统移动通信发展范式,在 6G 设计之初就用创新的理论和技术架构探讨支撑一体两翼、双轮驱动的新发展范式,谋求通信性能和安全可靠之间良好的平衡.

其次,美欧日等政府和科研机构也纷纷把安全、弹性、可信赖等广义安全概念列为 6G 的核心愿景和早期启动的项目清单.美国发布了面向 NextG 网络(包括 6G 蜂窝、未来版本的 WiFi、卫星网络)的 RINGS (Resilient & Intelligent NextG Systems) 项目计划,核心是强调发展网络弹性,包括安全性、适应性和自主性等,同时在其项目指南中,强制要求申请单位必须开展面向 NextG 的使能技术群(无线、频谱、网络等)和弹性技术群(安全、自适应和自主等)双轮驱动的协同融合创新,不接受单轮驱动的申请.欧盟 6G 旗舰项目 Hexa-X 提出要构建值得信赖(Trustworthiness)的 6G,要求确保端到端通信的机密性、完整性和可用性,保护数据隐私,保障网络运行弹性和安全性.日本通信部发布的 B5G 发展战略提出 2030 社会愿景是可靠的(dependable)、包容的和可持续的,B5G 需具备超安全性和弹性.

在此背景下,《中国科学:信息科学》组织出版了“6G 网络安全专题”,经过高质量、高效率的同行评议,共录用了 6 篇学术论文,涵盖 6G 内生安全新范式、体系架构与关键技术等.

“网络空间内生安全发展范式”,邬江兴院士围绕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,提出了解决问题的新理论和新方法论,以期用内生安全发展新范式为网络空间安全领域以及 6G 等新一代信息技术贡献可复制的成功模板.

“6G 网络内生安全架构研究”,分析研究了 6G 网络内生安全需求与安全能力演进趋势,设计了一种 6G 网络内生安全架构,并对内生安全体系的下一步发展与应用进行了分析与展望.

“混合窃听环境下多波束符号级安全传输方法”,针对混合窃听环境下多目标毫米波通信系统,基于阵列收发结构,提出了一种人工噪声辅助的多波束符号级安全传输方法,以实现混合窃听环境下无线安全传输.

“衰落高斯 MIMO 窃听信道下安全发送方案及其优化问题”,研究了合法用户信道状态随机衰落,且各状态不满足退化关系的高斯多天线输入输出(MIMO)窃听信道下的安全传输问题,提出了一种不依赖于信道状态信息的物理层安全传输方案.

引用格式:季新生,陶小峰,刘斐,等. 6G 网络安全专题编者按. 中国科学:信息科学, 2022, 52: 187-188, doi: 10.1360/SSI-2022-0012

“静态场景下基于 RIS 天线的物理层密钥生成方案”, 针对静态无线环境下密钥容量低的问题, 首次将可重构智能表面 (RIS) 天线配置在基站设备端用于密钥生成, 给出了通信安全联合设计方案, 实现通信与安全性能联合提升.

“面向 6G 流量监控: 基于图神经网络的加密恶意流量检测方法”, 针对 6G 网络正常与异常流量的边界模糊问题, 提出了一种基于图神经网络的加密恶意流量检测方法, 以实现加密恶意流量的高效检测.

受篇幅所限, 还有很多优秀的创新成果未能收入. 感谢所有作者的积极投稿和认真撰写, 感谢各位匿名评审专家细致认真的评审, 以及各位特约编辑的认真组织 and 无私付出. 最后, 希望本次专题能对 6G 安全理论、架构模型及关键技术研究起到积极推动作用, 对构建 6G 安全发展新范式有所贡献.

**特约编辑:** 季新生 网络通信与安全紫金山实验室  
陶小峰 北京邮电大学  
刘 斐 华为技术有限公司  
黄开枝 国家数字交换系统工程技术研究中心  
王慧明 西安交通大学  
李 娜 北京邮电大学