6G网络安全新需求及关键技术研究

Research on New Requirements and Key Technologies for 6G Network Security

谢泽铖[1,2],张曼君[1,2],徐　雷[1,2],姚　戈[1,2],谢中怀[1,2](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)

Xie Zecheng[1,2],Zhang Manjun[1,2],Xu Lei[1,2],Yao Ge[1,2],Xie Zhonghuai[1,2](1. China Unicom Research Institute,Beijing 100048,China;2. Next Generation Internet Broadband Service Application National Engineering Research Center,Beijing 100048,China)

摘　要:

ITU提出了6G网络"沉浸式通信、极高可靠低时延通信、极大规模通信、泛在连接、通信智能一体化、通信感知一体化"六大场景,带来了新的安全需求和挑战,需要融合新的安全关键技术来保障6G网络和业务的安全可靠。分析了ITU六大场景的安全需求,对物理层安全、隐私保护、轻量化接入认证、分布式认证、新型密码、安全智能编排、AI内生安全、AI赋能安全等可能应用到6G网络中的安全关键技术进行了探讨,并对后续6G网络安全研究工作给出了建议。

关键词:

6G网络;安全需求;安全关键技术

doi:10.12045/j.issn.1007-3043.2024.08.010

文章编号:1007-3043(2024)08-0049-04

中图分类号:TN929.5

文献标识码:A

开放科学(资源服务)标识码(OSID):

Abstract:

ITU defines six usage scenarios for 6G networks: Immersive Communication, Hyper Reliable and Low-Latency Communication, Massive Communication, Ubiquitous Connectivity, Artificial Intelligence and Communication, Integrated Sensing and Communication, which brings new security requirements and challenges. New security technologies need to be integrated to ensure the security and reliability of 6G networks and services. It analyzes the security requirements of ITU's six usage scenarios, discusses the key security technologies that may be applied to 6G networks, such as physical layer security, privacy protection, lightweight access authentication, distributed authentication, new cryptography, intelligent security orchestration, AI endogenous security, and AI enabled security. Finally, suggestions for the following research about 6G network security are given.

Keywords:

6G network;Security requirements;Security technologies

引用格式:谢泽铖,张曼君,徐雷,等. 6G网络安全新需求及关键技术研究[J]. 邮电设计技术,2024(8):49-52.

1 概述

目前,全球主要国家和相关研究机构均在积极推进6G研发及战略布局,ITU、3GPP等国际标准组织也在积极布局开展6G网络的愿景与标准制定工作[1-5]。2023年ITU-R审议通过了《Framework and overall objectives of the future development of IMT for 2030 and beyond》[6],定义了6G网络的"沉浸式通信、极高可靠低时延通信、极大规模通信、泛在连接、通信智能一体化、通信感知一体化"六大场景。其中沉浸式通信、极高可靠低时延通信和极大规模通信3个场景是对5G网络中增强移动宽带、大规模机器类通信和超可靠低延迟通信三大核心应用场景的增强,旨在提高数据速率、区域流量、连接密度、时延和可靠性等方面的要求;而泛在连接、通信智能一体化和通信感知一体化是ITU定义的3个新场景,旨在引入人工智能、通信感知等新技术,满足业务发展以及构建天地融合立体化网络的要求。这些增强和扩展的业务场景给6G网络带来了新的安全挑战和需求,因此在6G网络的设计阶段就需要充分考虑到这些新的安全需求,通过安全关

收稿日期:2024-06-17

键技术的部署应用来保障网络的安全和稳定运行。

2 6G六大场景的安全需求

2.1 沉浸式通信（Immersive Communication）

沉浸式通信场景扩展了5G现有的eMBB场景，不仅包括为用户提供沉浸式交互体验的场景，也包括为用户提供机器界面交互的场景，例如沉浸式扩展现实（Extended Reality，XR）、远程多感官呈现和全息通信等用例。在沉浸式通信场景下，网络中所传输的信息可能涉及用户人脸、声音等生物特征以及行为数据等其他敏感信息，需要确保这些数据在传输和处理过程中不被未经授权的人获取和篡改，避免隐私泄露风险；同时此场景下传输的数据量相较于其他业务更大，需要加解密速度更快的密码算法和流程，保障大通量数据的快速加解密。

2.2 极高可靠低时延通信（Hyper Reliable and Low-Latency Communication）

极高可靠低时延通信扩展了5G现有的uRLLC场景，其端到端时延将小于1 ms，典型场景包括智慧交互、工业控制、远程医疗等。由于这类应用本身关系到人身安全或高额经济利益，因此保障这类应用的安全至关重要，6G网络应采取更高级别的安全措施，且不能额外增加通信时延，而传统网络架构中采用的补丁式和外挂式防护措施，往往会降低传输效率，进一步加剧低时延与高安全性之间的矛盾。因此，对内生的安全机制、空口协议栈底层即可实现的安全机制、在端到端传输的各个环节进行安全机制的优化等方面提出了更高的要求，从而保障6G网络的传输效率，降低网络时延。

2.3 极大规模通信（Massive Communication）

极大规模通信扩展了5G现有的mMTC场景，带来的变化主要包括连接密度提升（将5G网络$10^6/km^2$的连接密度[7]提高到10^6~$10^8/km^2$）[6]以及物联网终端类型的丰富多样（例如引入免电池或极小电池并且从环境中获取能量的零功耗终端）。由于终端设备形态各异，其计算、存储、所能支持的安全能力不同，在6G网络中统一的安全方案不再适用。对于无源/半无源物联网等设备，传统加密、认证协议在终端侧存在复杂度高、安全强度不足等问题，需要引入轻量级的密码算法、设计轻量接入认证机制和简单高效的安全协议。

2.4 泛在连接（Ubiquitous Connectivity）

泛在连接是6G网络中的新场景，包含基于6G网络实现各种物联网设备、传感器和系统之间的无缝连接，也包含与卫星网络、行业网络、体域网等异构网络的连接。泛在连接场景下存在多种类型的通信设备和技术，具有跨行业及生态各方深度参与的特点，频谱、算力等资源将成为可由多方动态、按需共享的网络资源，来自不同组织机构的设备之间需要建立安全、可靠的信任关系。因此，需要一个去中心化、公开透明、不可篡改的运行机制，能够凝聚多方共识，处理资源竞争问题，使得整个过程公开透明、真实可信。

2.5 通信智能一体化（Artificial Intelligence and Communication）

通信智能一体化是6G网络中的新场景，AI技术与无线通信相互融合，实现了网络的智能化与高效化，其核心特点在于AI算法与传统的无线通信技术之间的深度集成与互补，使得整个网络不仅能够以前所未有的效率和灵活性处理数据，还能够实时适应环境变化和用户需求的变动[8]。AI被引入移动通信网络后，攻击者可通过投放病毒数据、输入异常噪声、设置模型后门、伪造合法数据等方式实现对AI模型本身的攻击，或者通过模型逆向和成员推理等攻击方式获取模型参数、训练数据等敏感信息，导致数据泄露，这需要确保训练数据的安全，以及保障算法模型的安全。

2.6 通信感知一体化（Integrated Sensing and Communication）

通信感知一体化是6G网络中的新场景，它使得网络具备感知功能，可以提供广域、多维度的感知能力，用于无人机监测、车联网、环境监测、数字孪生等以传感信息为基础的应用场景[9]。这些场景往往要求网络支持高精度的定位，并能够准确对物理对象的某些参数进行捕捉和感知，涉及到大量用户隐私数据，例如智能家居中的用户影像、个人习惯等隐私信息；智慧交通中车辆运行轨迹、位置等隐私信息；环境监测获取的气象数据等隐私信息，而这些数据在采集、存储和传输中存在隐私暴露和非法使用的风险，对核心网侧处理通信感知数据的相关网元[9]提出了更高的要求，不仅要完成业务授权、感知数据接收与计算，还要针对敏感数据进行隐私保护处理，并且确保感知数据开放给可信的第三方。

3 6G安全关键技术

6G安全关键技术是满足6G六大场景安全需求的

技术基础，依托传统安全技术的演进和新兴安全关键技术的应用，结合6G网络中无处不在的算力资源和数据资源，将为安全关键技术的进一步发展和应用提供可能。未来可能应用于6G网络的安全关键技术如图1所示，包括物理层安全、隐私保护、轻量化接入认证、分布式认证、新型密码、安全智能编排、AI内生安全、AI赋能安全等。

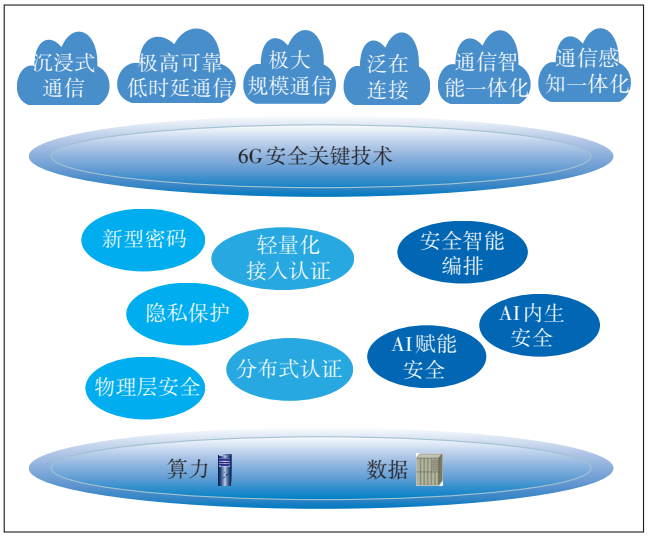

图1　6G安全关键技术示意

3.1 物理层安全

物理层安全技术与窃听者的计算能力无关，基于无线信号多径衰落、时变性、互易性和去相关性等四大特征，利用合法信道和窃听信道的差异性生成密钥和处理发射信号，在提高无线传输安全性、无线信道密钥生成、身份认证中均可应用。结合智能超表面（Reconfigurable Intelligence Surface，RIS）技术来构造快变信道，可以增加信道的随机时变性，提升密钥生成性能。物理层安全技术属于在空口协议栈底层即可实现的安全机制，可减少与高层协议间的消息交互，满足极高可靠低时延通信场景对于保障安全性和减少传输时延的需求。

3.2 隐私保护

基于数据加密、个人信息去标识化、脱敏保护、多方计算、同态加密等技术，可在数据传输、使用过程中隐藏用户隐私信息，实现用户信息的“可用而不可见”，从而有效避免敏感信息泄露。依据底层、高层、应用层等不同层中不同节点的隐私保护能力，可以设计不同级别的隐私保护方案，例如在不同信任域内提供不同的半永久或者临时标识，由核心网网元提供不同标识的映射、查询、动态更新等管理服务，位于低信任区域的用户只能使用生命周期比较短的临时标识，从而增强身份的隐私保护。隐私保护相关技术可以满足沉浸式通信、通信感知一体化场景对重要数据和敏感数据进行安全保护的要求。

3.3 轻量化接入认证

设计轻量级接入认证协议和流程，实现多认证体制下海量6G网络设备和用户的跨域随机接入，如在现有用户接入基础上，采用轻量化的密码算法、简化认证流程、压缩协议字段、减少交互次数或密钥层级，降低安全协议复杂度；对于无源/半无源等A-IoT设备，引入单向认证、默认安全算法配置而无需安全能力协商流程等。通过轻量化的接入认证技术，可以减少包括业务接入过程中身份认证、安全上下文切换等流程带来的时延，解决极大规模通信场景下大量低能力终端的安全接入问题。

3.4 分布式认证

分布式认证可采用基于共识的信任模式以及采用数字身份技术实现。其中基于共识的信任模式将区块链与身份认证相结合，利用分布式账本的公开透明、多方共识、不可篡改的特性构建信任联盟，实现基于分布式账本的证书和身份管理、透明审计和跨域验证[10]；数字身份技术使得用户可以自主掌控身份在不同信任域或业务中的使用范围，选择性地分享特定的身份信息给需要验证的实体，并将身份认证拓展到网络中的所有主体。分布式认证相关技术使得信任根不再依赖于集中的单点，可满足泛在连接场景下跨行业、跨子网的多方认证互信需求。

3.5 新型密码

后量子密码、轻量化密码等新型密码相关技术为完善6G网络密码体系提供了可能，包括ASCON、ISAP等NIST公布的轻量化密码算法以及CL-PKC、IPK等其他轻量化密码算法在6G网络中的应用，量子密钥分发（Quantum Key Distribution，QKD）在6G网络密钥派生体系中的应用，256 bit密钥长度的对称密码算法以及其他非对称后量子密码（Post-quantum Cryptography，PQC）在6G网络中的应用。轻量化的密码算法可减少资源开销和对硬件的依赖，QDK、PQC可应对量子计算对现有移动通信网络密码学体系带来的冲击，保障6G网络中数据的传输、存储、处理安全。

3.6 安全智能编排

将物理及虚拟的网络安全设备与其接入模式、部

署方式、实现功能进行解耦，底层抽象为安全资源池里的资源，顶层融合AI技术和软件定义安全技术，统一通过软件编程的方式进行智能化、自动化的业务编排和管理。通过安全智能编排相关技术，构建统一的智能安全分析和编排调度，使得网络安全能力能够动态适配异构网络、多样化的终端环境和复杂的业务场景，实现快速调度和弹性部署，进行网络安全能力的智能化全网调度分配以及对外的自动化编排输出，从而保障业务的连续性和安全性，满足6G多场景下的差异化安全保护需求。

3.7 AI内生安全

AI面临着训练数据和模型算法的安全风险，对于训练数据的安全防护，可采用先进的隐私保护技术，在不泄露个人信息的前提下，对大量数据进行分析和处理，在安全的环境下完成模型的联合训练、更新和推理；对于保障算法模型的安全防护，可开发高效的安全攻击检测和防御机制，使用对抗性训练方法来增强模型对攻击的鲁棒性。通过AI内生安全技术，解决了通信智能一体化场景下，将AI引入移动通信网络后带来的新的安全挑战。

3.8 AI赋能安全

AI赋能安全为保障6G网络安全提供了更多的技术手段，例如利用AI自动识别或响应潜在网络威胁，通过对网络数据、业务数据、用户数据等多维数据感知学习，对攻击行为和威胁情报进行建模或特征提取，检测识别已知或未知恶意软件，分析和溯源网络攻击行为，提高通信系统安全自主自治能力。利用AI能力积极赋能安全，使得6G网络具备自我检测和自我修复的能力，在受到攻击时能够及时发现异常并进行自我修复，确保业务的持续运行。

4 结束语

未来的6G网络将引入卫星网络、通信感知一体化、数字孪生网络等新型异构网络，以及沉浸式XR、全息通信等虚拟化与现实相结合的新业务，将深入渗透到交通、医疗、工业等各个领域，为改变人类社会做出更为积极的贡献[11]。在后续6G安全关键技术的研究过程中，需要关注相关技术和方案对6G网络性能、成本、用户体验等的影响，寻求网络安全与网络性能之间的平衡，既要保障网络安全，又要避免引入安全技术而影响网络的性能。

总之，6G安全必须根据新场景、新架构的特点，不断完善密码算法和网络安全机制，创新网络安全管理策略和工具，采用一系列创新的安全关键技术和解决方案，才能在享受6G网络带来的便利同时，保障下一代移动通信系统的安全性和可靠性。

参考文献：

[1] FG-NET-2030. A blueprint of technology, applications and market drivers towards the year 2030 and beyond[R/OL]. [2024-01-08]. https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf.

[2] YLIANTTILA M, KANTOLA R, GURTOV A, et al. 6G white paper: research challenges for trust, security and privacy[R/OL]. [2024-01-08]. https://arxiv.org/abs/2004.11665.

[3] IMT-2030(6G)推进组. 6G总体愿景与潜在关键技术白皮书[R/OL]. [2024-01-08]. https://blog.csdn.net/qq_37857219/article/details/117736024.

[4] 中国联通研究院. 中国联通6G白皮书(V1.0)[R/OL]. [2024-01-08]. http://221.179.172.81/images/20210322/30691616408868127.pdf.

[5] 大唐移动通信有限公司. 全域覆盖，场景智联：6G愿景与技术趋势白皮书(V.2020)[R/OL]. [2024-01-08]. https://www.docin.com/p-2570258581.html.

[6] ITU. Framework and overall objectives of the future development of IMT for 2030 and beyon[EB/OL]. [2024-01-08]. https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en.

[7] ITU-R. ITU-R M.2083-0 建议书，IMT愿景-2020年及之后IMT未来发展的框架和总体目标[R/OL]. [2024-01-08]. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M. 2083-0-201509-I!! PDF-C.pdf.

[8] IMT-2030(6G)推进组. 无线人工智能(AI)技术研究报告[R/OL]. [2024-01-08]. http://doc. cserver. com. cn/doc_0a05234e-4420-474a-81f3-e4c822a85ba3.html.

[9] IMT-2030(6G)推进组. 6G通感融合系统设计研究报告[R/OL]. [2024-01-08]. https://www.imt2030.org.cn/html//default/zhongwen/xinwendongtai/1718878960697274369.html?index=4.

[10] ETSI. Permissioned Distributed Ledgers (PDL); overview of use cases in 3GPP network and impact analysis on architecture integration: ETSI - GR PDL 021[S/OL]. [2024-01-08]. https://standards.globalspec.com/std/14636536/gr-pdl-021.

[11] IMT-2030(6G)推进组.《6G典型场景和关键能力》白皮书[R/OL]. [2024-01-08]. https://www. bita. org. cn/newsinfo/3130433.html.

作者简介：
谢泽铖，工程师，硕士，主要从事网络与信息安全研究工作；张曼君，正高级工程师，博士，主要从事网络与信息安全研究工作；徐雷，教授级高级工程师，博士，主要从事网络与信息安全研究工作；姚戈，工程师，博士，主要从事网络与信息安全研究工作；谢中怀，工程师，硕士，主要从事网络与信息安全研究工作。