引用格式:张平. 无线数字新技术及网络数据安全[J]. 信息对抗技术,2024, 3(2):1-4. [ZHANG Ping. New wireless digital technology and network data security[J]. Information Countermeasure Technology, 2024, 3(2):1-4. (in Chinese)]

特 邀 评 述

无线数字新技术及网络数据安全

张 平

(北京邮电大学,北京 100876)

摘 要 当前,以第六代移动通信技术(6th-generation mobile communication tenchnology, 6G)为代表的无线数字新技术正在塑造着这个信息新时代,在积极发展并应用这些技术的同时,必须高度重视网络数据安全。为此,就网络通信发展态势、6G 演进及数据安全、网络数据安全及挑战进行简要评述。

关键词 无线数字新技术;6G;数据安全

中图分类号 TP 385 : TP 393.08 **文章编号** 2097-163X(2024)02-0001-04

文献标志码 A **DOI** 10.12399/j.issn.2097-163x.2024.02.001

New wireless digital technology and network data security

ZHANG Ping

(Beijing University of Posts and Telecommunications, Beijing 100876)

Abstract Currently, new wireless digital technology represented by 6th-generation mobile communication tenchnology(6G) are shaping this new information age. While actively developing and applying the technology, we must pay much attention to network data security. This article briefly reviewed the development trends of network communication, 6G evolution and data security, and network data security and challenges.

Keywords new wireless digital technology; 6G; data security

0 引言

无线数字新技术的发展给当今世界带来了 3 大课题:一是 6G 的发展;二是其引起的数据安全;三是网络数据安全及应对。迄今,互联网的演进历经了由 Web 1.0 到 Web 3.0 这 3 个过程,其中,Web 1.0 是可读式,Web 2.0 是交互式,Web 3.0 则是共同参与模式。在区块链出现之后,互联网的发展趋势呈现为去中心化,其发展方向有 3 个,其中之一就是终端技术,例如:Web 1.0 的台式、Web 2.0 的智能式、Web 3.0 的增强现实(augmented reality, AR)和虚拟现实(virtual reality, VR)。AR 和 VR 是未来 6G 的主要应用,需要强大的算力支持,而算力的发展趋势是从传统的数据中心到云计算、区块链、算力网络、可信计算以及跨链的计算。未来在算力网络的支撑下,人工智能(artificial intelligence, AI)必然会朝着强 AI 的方向发展,信息的形态也会由一维到二维,再到三维全景,最后演变为五感真实。这其实也是无线数字新技术发展的一个线路图。然而,当这些发展倚重于依靠网络构建的数字新技术时,如何保障数据安全也就成为一个无法回

收稿日期:2024-01-08 **修回日期**:2024-03-11

避的问题。

1 网络通信发展态势

虽然未来有量子通信，但经历了 50 多年的传统信息通信网络仍然是当下主要的通信方式。目前，为了在 6G 发展中取得技术优势，大国之间正在围绕互联网平台、合成生物、生物医药、聚变能源、量子计算、先进电池、5G 通信、无人机等方面展开激烈竞争。

在国际上，美国企图在 6G 阶段重树领导地位，主导欧美阵营 Next-G/6G 联盟，并且以安全为名打压他国通信产业；日本的 6G 标准专利在世界上占比达 10%，其电信运营商 NipponTelegraph & Telephone（NTT）计划利用 6G 试验网为 2025 年的大阪世博会提供服务；欧盟也希望引领未来 6G 网络发展，启动若干 6G 项目及平台建设，并采用种种策略把他国排斥在外，但其产业受到美国牵制。其实，这种竞争格局在 3G 阶段就已经存在。

面对当前的国际局势，我国必须着手开放云化网络。云化网络就是把过去固有的协议变成一些设备，做垂直整合、水平开放共享。在这方面，关键技术有望突破的时间窗口是 2023—2026 年，这方面需要做好标准征集及评估。

当前，我国率先启动 6G 的研发布局，先后成立了技术研发推进工作组、总体专家组、IMT-2030（6G）推进组等专门机构。一些运营商相继发布了 6G 网络整体架构及关键技术研究成果；中国移动打造了 6G 协同创新基地，完成了 6 项技术原型样机；设备商华为、中兴、中信科移动的 6G 研发工作进入关键技术概念样机阶段。此外，鹏城实验室和 IMT-2030（6G）推进组研发了面向 6G 的无线高速接入原型系统及测试环境——EAGLE 6G；紫金山实验室研发了 6G TKμ 极致连接无线传输试验平台 V 1.0；中关村泛联移动通信技术创新应用研究院研发了 6G 云化无线网络开放试验平台；等等。

与计算机遇到的智能问题有所不同，通信领域的智能就是添加增量，IMT-2030（6G）增加了 6 项能力（沉浸式、AI 和通信一体化、超可靠低延迟通信、泛在连接、超大规模链接、感知通信一体化），其中，安全、隐私、韧性、泛在智能、可持续性是未来 6G 发展面临的最主要的任务。

在网络的技术应用领域，我国走在了世界前列，如腾讯、百度、阿里巴巴以及其他移动互联网得到了普及应用。下一步需要整合科技创新资源，强化我国信息通信产业已有的优势。然而，目前存在的问题也比较多，主要是缺乏影响网络通信技术方向长远发展的原创性基础理论以及颠覆性技术创新，同一领域各自为战，缺乏交叉融合、协同研究的创新；在基础材料、关键元器件、系统软件、工艺和生态环境建设等方面，核心技术掌握相对不足，受遏制明显，不利于支撑产业发展。此外，对于基站漏洞挖掘、数据安全保护技术也需要进一步加强。因此，必须在补“短板”的基础上，进一步加强基础研究和核心技术研发、5G/6G 网络及应用、数据安全技术研究，在国际竞争中取得优势，建立“长板”。

2 6G 演进及数据安全

2.1 AI 赋能通信

6G 是有增量的，这个增量需要面向整个社会的发展，需要把 AI 大模型通过现在信道的恶劣环境贯穿式发展起来。5G 时期，窄带物联网（narrow band Internet of Things，NB-IoT）的接入研发比较困难，目前使用大规模机器类通信（massive machine-type communications，mMTC）进行代替。NB-IoT 实际上是 4G 技术，若不与 AI 和 6G 通信相结合，而只是单纯地分析模块，就不能算是真正的 AI。

5G 网络是人-机-物的万物互联，而 6G 则进一步拓展了网络空间。过去，网络空间是指社会空间、信息空间和物理空间，5G 是人、机、物的连接，而 6G 则是人、机、物和智慧体的连接，这种智慧体是高级智能体，能够辅助决策。过去的通信是把信息从甲地搬移到乙地，满足可靠、数量足够大、足够安全等要求即可。然而，伴随着大量无人机的出现，通信需要跟人一样具有决策功能，成为一个智慧体，这就是 AI 赋能通信的结果。

2.2 6G 数据安全

当前，网络的数据安全已被列入国家层面的 6G 网络发展规划中。这需要跟 AI 的发展结合起来。AI 算法不同，变化就会不同，因此涉及的数据安全就需要“道高一尺，魔高一丈”。“安全”永远在路上，然而没有一个方法能够有效解

决所有的安全问题,所以这里更加关注的应该是解决问题的反应时间。

6G 网络数据安全技术的未来发展趋势,是需要深度思考的,应重点关注强化学习、认知图谱、智能决策、可解释性 AI 等方向的发展。随着与垂直行业的深度融合,6G 一方面将赋能万物智联、数字孪生愿景,另一方面也会面临诸多安全风险,包括多样化终端的安全风险、网络能力开放面临的安全风险、网络切片的安全风险、基础设施虚拟化云化的安全风险、保密通信风险、边缘计算风险、AI 层面的安全风险、大数据层面的安全风险,等等。未来,我国需要加强数字核心技术攻关,重视信息基础设施及安全,实现大平台支撑;深入实施创新驱动发展战略,着力完善创新布局、优化创新环境、聚焦网络安全要素,推动科技成果转化应用,坚持把科技创新摆在更加突出的位置,切实加大科技创新、科技应用、科技成果的转化力度,更好地赋能中国经济长治久安和高质量发展。

3　网络数据安全及挑战

数据安全威胁具有严重后果,具体表现为:

1) 造成社会信任危机。如患者的隐私被暴露,医疗数据的不安全使用,智慧医疗数据的保护不到位,等等。现在大数据做的很多工作能够让数据自由流转,产生价值,成为社会经济增长的一个新要素,但是,如果无法建立信任,将会带来很多问题。

2) 造成社会事件冲击。如社会暴乱以及个人快递信息的大规模泛滥,都可能会造成社会事件的冲击。

3) 滥用基础设施及核心数据。如城市地理信息和商业信息的泄露,必然会损害国家、集体和个人的安全、利益等。

3.1　信息网络数据安全分类

信息网络数据安全可以分为业务数据安全和用户隐私数据安全,其中,业务数据安全表现在数据的传输安全、数据传输的可靠以及网络管控的安全;用户隐私数据安全表现在安全存储、敏感数据的安全共享、数据价值的安全挖掘。这样的分类能够涵盖控制数据安全、用户数据安全和大数据的使用安全这 3 个层面。

3.2　业务数据安全与挑战

业务数据的安全需求,一方面体现在智享生活中,例如,扩展现实(extended reality, XR)业务需求端到端的时延小于 10 ms;全息通信需要打通虚拟与现实场景界限,提供沉浸式服务,且吞吐量达到 TB 级;感官的互联互通,即视觉、听觉、触觉、嗅觉、味觉等全感官的互联通信需要能够反馈定位精度及用户数据隐私;智慧交互,要求时延低于 1 ms,而且可靠性达 99.999%。另一方面体现在智赋生产及智焕社会中,例如,普惠智能的智能车、智能机器人等智能体不断学习、合作,智慧决策与物理世界不断融合。网络需求是网络群体智慧能力的体现,需保证数据协作、数据安全共享。通信感知一体化体现在挖掘毫米波、太赫兹高频段能力,实现通信感知一体化的高精度环境感知。网络需求对通信感知一体化信号设计及通信感知一体化环境数据安全提出了更高的要求。数字孪生体现在物理世界在数字世界的镜像孪生,数字世界对物理过程的模拟、验证、控制。网络需求为亿万级设备海量连接,及亚毫秒级时延、数据安全。

业务数据安全面临着诸多挑战,包括:1) 工业互联网、自动驾驶、智慧医疗等垂直行业应用对未来网络发展提出的新需求,即克服低时延高可靠环境的数据安全保护与共享方面的技术难题;2) 物联网海量终端设备能力差异大,移动终端差异化增加了终端被攻击概率,网络间差异化的“安全衔接”扩大了被攻击面,这是另一个重大挑战。

3.3　用户隐私数据安全与挑战

用户隐私数据安全需求具体体现在 2 个方面:1) 数据流动的价值。经济上跨行业重构用户画像,如银行机构、大数据用户认证、企业广告投放等;智慧医疗上的数据互通,如疫情防控精准筛查、全基因组联合分析、临床疾病预测等;电子政务上的数据开放共享,如部门政务数据安全共享、税务智能审计及部门、企业数据融合等。2) 隐私数据的安全存储。例如,2020 年 4 月,亚马逊泄漏了 7.6 万份美国能源行业用户的数据。2021 年 4 月,5.33 亿个 Facebook 数据遭到泄露,包括姓名、住址、出生日期以及简历等大量隐私

信息。

用户隐私数据安全面临的挑战包括：1）机器网络空间对抗。由于 5G/6G 时代通信的主体是机器，因此亟须从机器的角度分析网络空间对抗行为，保障复杂系统数据隐私。例如，物联网（Internet of Things，IoT）数据的模式数量很大，在 2018 年达到 91 亿，预计 2025 年将会猛增至 252 亿，这是一个复杂的巨系统对抗，需要对行为进行分析。2）海量差异化数据。海量移动互联网数据具有差异化隐私需求，亟须解决海量数据安全难题，并根据隐私需求进行可定制化的数据安全服务。

总之，无线数字新技术是信息技术发展的必然结果，巨大的社会需求是其发展的原动力，它正以不可逆转之势快速发展；同时，其发展也不可避免地伴生着巨大的网络安全威胁，这就要求我们必须在数据安全审计、数据安全共享、数据可信交互等方面积极应对。

作 者 简 介

张 平

男，1959 年生，中国工程院院士，教授，博士研究生导师，网络与交换技术国家重点实验室主任，鹏城实验室宽带通信部主任，中关村泛联移动通信技术创新应用研究院院长，《通信学报》主编，IEEE 会员。研究方向为语义通信和语用达意网络。长期致力于移动通信理论研究和技术创新，担任 IMT-2020（5G）专家组成员、IMT-2030（6G）推进组咨询委员会委员。曾获国家科学技术进步奖特等奖等多项奖励，为推动我国自主技术成为国际主流做出了基础性的贡献。

E-mail：pzhang@bupt.edu.cn

责任编辑 钱 静