5G/5G-Advanced/6G接入网安全技术演进及内生安全

Security Technology Evolution and Intrinsic Security of 5G/5G-Advanced/6G Access Network

陆海涛/LU Haitao[1,2,3]，陈一喆/CHEN Yizhe[4]，娄笃仕/LOU Dushi[1,3]
（1. 中兴通讯股份有限公司，中国 深圳 518057；
2. 深圳市无线移动技术重点企业研究院（中兴），中国 深圳 518055；
3. 深圳市5G接入网安全技术研究及应用重点实验室，中国 深圳 518055；
4. 南京邮电大学，中国 南京 210003）
(1. ZTE Corporation, Shenzhen 518057, China;
2. Shenzhen Key Enterprise R&D Institute of Wireless Mobile Technology (ZTE), Shenzhen 518055, China;
3. Shenzhen Key Laboratory of 5G RAN Security Technology Research and Application, Shenzhen 518055, China;
4. Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

DOI：10.12142/ZTETJ.202206014
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221219.1255.001.html
网络出版日期：2022-12-20
收稿日期：2022-10-08

摘要：网络安全技术在无线通信技术的演进中不断增强。介绍了现有5G网络的安全技术方案，并结合5G行业应用需求，探讨了5G-Advanced增强安全技术。立足于万物智能互联愿景，从海量设备连接、智能运维、人工智能/机器学习、区块链方面分析了内生安全技术。认为内生安全是6G网络安全研究的热点，轻量化是6G内生安全的主要特征之一。

关键词：内生安全；行业应用；物联网；海量连接；轻量化

Abstract: Network security technologies are constantly enhanced in the evolution of wireless communication technology. The security technology solutions of the existing 5G networks are introduced, and the 5G-advanced enhanced security technologies are discussed in combination with the 5G industry application requirements. Based on the vision of intelligent interconnection of everything, the intrinsic security technologies are analyzed from the aspects of massive equipment connection, intelligent operation and maintenance, artificial intelligence/machine learning, and blockchain. It is considered that intrinsic security is the focus of 6G network security research, and lightweight is one of the main features of 6G intrinsic security.

Keywords: intrinsic security; industry application; Internet of Things; massive connections; lightweight

第3代合作伙伴计划（3GPP）定义了5G的三大应用场景：增强移动宽带（eMBB）、超可靠低时延通信（URLLC）和海量机器类通信（mMTC）。3GPP在制定5G网络标准时已把安全性作为核心问题来考虑，并在5G的第一个标准R15里提出5G网络安全架构[1]，从访问域、网络域、服务化架构（SBA）域等方面分别定义了安全功能和组件。3GPP R15标准于2018年6月被冻结，该标准主要规定了eMBB和URLLC两大场景。基于3GPP R15的网络安全架构，文献[2]针对5G接入网和基站设备，从基础设施、新空口（NR）、核心网接口和网管接口4个方面提出了安全解决方案。

基金项目：广东省重点领域研发计划（2020B0101120003）

2020年7月3GPP R16标准被冻结，该标准完善了URLLC技术特性。该技术特性使得5G可以应用于工业、港口、地铁等物联网中，为5G面向企业（ToB）垂直行业应用打下基础。此时业界开始意识到：传统的网络安全防护机制是“外挂式”“补丁式”的，难以应对未来万物互联所面临的安全挑战，因此需要改变传统的安全防御思想，不再使用独立安全解决方案来应对安全问题，需要重新设计安全协议和机制，建立一套完备的信息系统安全体系，使系统具备自我免疫、内外兼修、自我进化的特点，从网络内部增强安全防范能力，从源头上抵制攻击的产生[3]，即实现内生安全。

2022年6月3GPP R17标准被冻结。该标准支持增强的工业物联网、精准授时、高精度定位和车联网（V2X），并

引入了面向较低复杂度物联网终端的RedCap，将5G扩展至几乎全部终端和用例，为实现5G万物互联提供了重要支撑。

3GPP在2022—2026年进行5G-Advanced标准（R18/R19/R20）的研究，并将在2027—2030年开展6G标准（R21/R22/R23）的研究，继续在移动宽带、固定无线接入、工业物联网、V2X、扩展现实（XR）、无人机与卫星接入等用例方面进行空口协议演进与增强，研究和制定更高频段的相关标准。另外，6G通信标准的服务范围将从陆地扩展到卫星、海底、地下，真正实现海、地、天三位一体通信。

1 5G接入网安全技术

5G通信网络由终端、接入网、承载网和核心网组成。其中，接入网是指用户终端和骨干承载网之间的设备和链路，可实现无线信号的接入和转换。5G接入网的关键设备是5G基站（gNB），可实现3GPP定义的5G协议规范，具有大带宽、高可靠低时延、多连接的特性。相关核心指标包括无线频谱效率、峰值速率、用户体验速率、流量密度、连接密度、时延和移动性等。5G接入网安全技术主要包括终端安全、空口安全、基础设施安全、安全日志和公钥基础设施（PKI）系统等，如图1所示。这些技术是5G基站为数据处理、协议转换、访问控制和管理功能提供的安全支撑和重要保障。

（1）终端安全

终端安全是指在用户接入网络时做认证和鉴权的控制，对用户身份进行确认。长期演进技术（LTE）/5G使用了全新的双向认证方式和配有用户识别模块（UIM）的全球用户识别卡（USIM）。只有都完成网络对终端认证和终端对网络认证后，用户才可接入网络。5G增加了5G认证与密钥协商协议（5G-AKA）认证，并通过向归属网络提供用户设备（UE）从访客网络成功认证的证明，来增强演进分组系统（EPS）-AKA的安全性[1]。

对5G基站而言，终端安全更侧重于用户隐私数据的保护。例如，欧盟的《通用数据保护条例》和中国的《中国个人信息保护法》都严格要求在收集个人数据之前要征得用户同意，并规定了收集和处理数据的义务和责任。

5G基站数据处理所涉及的用户隐私数据有两种：一是执行3GPP协议处理所涉及的协议消息内容，如用户永久标识（SUPI）/国际移动用户标识（IMSI）、用户匿名标识（SUCI）、5G全球唯一临时标识（5G-GUTI）/临时移动用户识别码（TMSI）、国际移动设备标识（IMEI）、用户互联网地址（UE IP）及位置区标识（LAI）定位信息等；二是操作维护管理所涉及的管理消息内容，如SUPI/IMSI、UE IP等。对于所涉及的用户隐私数据，5G基站通过采取数据加密、系统加固、数据脱敏等措施来保护隐私数据的安全。

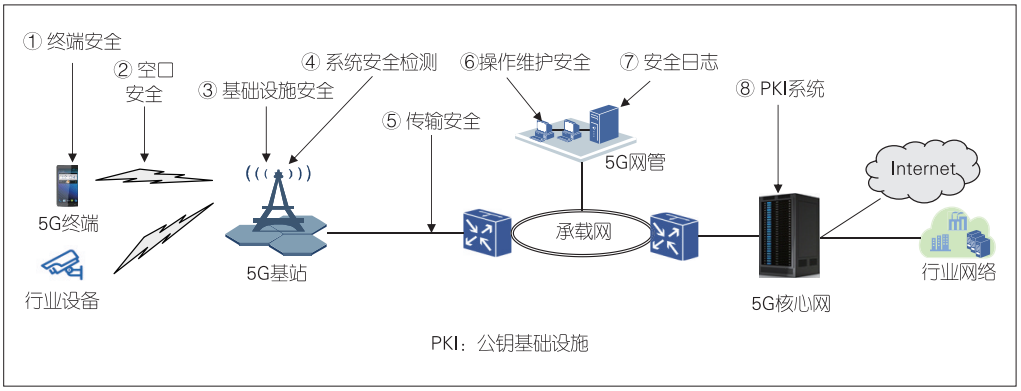
（2）空口安全

空口安全主要解决终端和基站之间无线通道的安全传输问题。由于无线信号覆盖在空间各处，非法用户可以随意截取，因此需要对空口数据进行加密和完整性保护，防止数据泄露或被篡改。

5G基站的空口安全处理包括数据加密和完整性保护。其中，数据加密是指发送方通过加密算法将明文数据转换为密文数据，保证数据不泄露；完整性保护是指发送方通过完整性算法计算出完整的消息认证码（MAC-I），接收方通过完整性算法计算预期的消息身份验证代码（X-MAC），并比较MAC-I和X-MAC是否一致，以保证数据不被篡改。5G基站在分组数据汇聚协议（PDCP）层实现数据加密和完整性保护功能，根据核心网发送的安全策略激活安全功能。加密算法由5G基站通过无线资源控制（RRC）信令发送给终端，密钥由终端和5G基站生成。

（3）基础设施安全

5G基站的基础设施安全包括多个方面。（a）物理设备安全：对基站以及周围设施保证安全，如设置门禁、监控，配备烟雾、温度传感器等；（b）操作系统安全：定期对软硬件进行安全威胁分析和评估，每发布一个软件版本，都需要经过第三方软件的安全扫描和评估，对于发现的漏洞和风险能够及时解决；（c）禁用不安全的服务和协议：与基站应用无关的操作系统（OS）服务和协议需要被关闭或移除，不使用的端口缺省也要被关掉，提供对外开放的端口/协议列表，支持端口/协议可关闭；



▲图1 5G接入网安全技术架构

（d）存储安全：本地存储的机密信息都需要加密，其中特别敏感的信息还要存放在保护区内；（e）不使用无支持的硬件和软件模块：在基站产品开发过程中，可选择硬件模块或者第三方软件模块，但不能选用已经没有支持和不再升级的产品，因为这类产品往往存在安全缺陷。如果没有支持来修补安全漏洞，基站就会暴露安全问题。

（4）系统安全检测

系统安全检测可保护基站正常运行，在软硬件异常或故障时能够快速恢复，避免基站服务中断。资源监控、回收、复位、告警、日志等手段可保证业务软件服务与硬件资源的可用性。（a）中央处理器（CPU）监控与死锁检测：通过线程切换等关键点的时刻记录来获取运行时间，计算线程在一个周期内的CPU占用率，结合线程的CPU/核占用率和主动切换次数，判断线程是否进入死循环或处于死锁状态，记录现场日志并恢复服务；（b）内存泄露检测：限定具体进程的内存使用量，结合申请者信息和一些使用策略对内存泄露做出判定，在监控到这些问题发生时记录详细的异常日志；（c）孤岛监控与自救：当各种故障与核心网、网管等连接设备断链出现孤岛状态时，系统会监控孤岛状态，实施自救，传输参数回滚等以保障基站服务的可用性。

（5）传输安全

传输安全主要指5G基站数据传输的安全协议保障，涉及5G基站之间、5G基站与LTE基站间的Xn/X2接口，5G基站与5G核心网及LTE核心网间的下一代5G（NG）/4G（S1）接口连接。传输网络协议涉及物理层到应用层之间的安全协议。如果这些接口的物理网络非可信，则需要通过连接安全网关（SeGW）建立端对端的安全通信隧道，支持Internet安全协议（IPSec），保证5G基站数据传输的安全。另外，基站和网管间的传输链路也要支持传输层安全（TLS）协议，保证管理数据的安全。

由于是一个多层次的需求，在某些特定场景中数据传输安全还需要支持更底层的业务，例如实现链路层的额外保护。相关协议包括电气与电子工程师协会（IEEE）制定的基于端口的访问控制和认证协议（IEEE 802.1x）、媒体访问控制安全（MACSec）协议等。

（6）操作维护安全

5G基站的操作维护安全涉及配置、版本、告警、诊断操作等。维护用户是指对基站进行配置、操作和维护的使用者，用户必须唯一识别。基站的操作维护系统功能包括SSH、SFTP和Web服务。授权用户可以通过基站的本地管理口从外部远程访问，非授权用户不能接入系统。用户接入系统后还需要进行权限控制，即用户能够读取/修改/执行系统文件是否在授权范围内。系统需要对用户分组，不同等级的用户分组有不同的用户权限。

系统支持集中账户管理和本地账户管理。其中，集中账户是指通过轻量目录访问协议（LDAP）等集中管理分布网元的账户，本地账户用于设备近端的操作维护管理。系统的用户访问控制是指对用户授权可以访问的对象和执行的操作，通常通过基于角色的权限分配来实现。

（7）安全日志

5G基站提供安全日志，记录用户登录和登出、用户权限变更等安全事件以供审计，提供有效证据防止人员或实体否认执行过的活动。同时基站实时反馈5G网络系统的安全势态，让运营商了解无线系统的整体安全情况，提供日志查询、安全事件关联分析和报告等。当分析结果有潜在和可疑的活动时，系统会产生告警并调查可疑活动。

（8）PKI系统

5G规范引入了基于PKI的安全体系结构。3GPP 33.310协议定义了基站数字证书的注册机制，以及应用数字证书与核心网建立安全通信链路的过程。PKI采用非对称密码算法技术实现可提供安全服务的具有通用性的安全基础设施，能够为所有网络应用提供采用加密和数字签名等密码服务所需要的密钥和证书管理，并提供创建、颁发、查询证书的功能。

设备商为基站提供出厂生成的公私钥对。基站会预装由设备商签名的数字证书、登记授权（RA）/证书授权（CA）服务器预装设备商根证书、核心网SEG预装运营商根证书。然后基站向核心网注册并使用证书管理协议版本2（CMPv2）协议向RA/CA发起证书申请。RA/CA则使用设备商根证书和设备商签名证书对基站进行身份验证。验证通过后基站会获得签发的运营商证书并返回证书响应。基站证书替换为运营商签名证书，则表明基站注册完成。随后基站使用运营商签名证书与核心网建立IPSec安全连接。

2 5G-Advanced安全增强技术

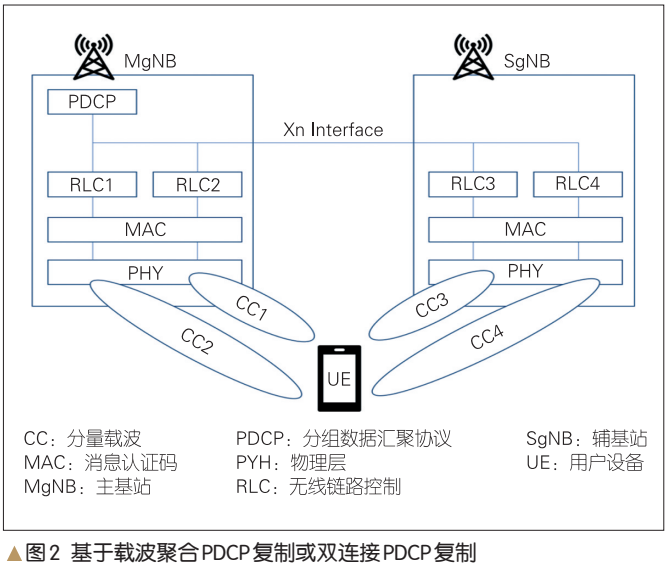
5G发展的关键是应用。2021年7月，工业和信息化部等十部门联合发布了《5G应用“扬帆”行动计划（2021—2023年）》，从5G应用标准体系、面向行业需求的5G产品、5G应用创新生态、5G应用安全能力四大领域打造5G融合应用新产品、新业态、新模式，为经济社会各领域的数字转型、智能升级、融合创新提供坚实支撑。中国5G应用市场发展空间巨大，根据行业互联网数据中心（IDC）研究预测，到2025年全球物联网市场将达到1.1万亿美元，其中中国市场占比将提升到25.9%，物联网市场规模全球第一。大部分市场增长来自企业市场，这说明5G发展将

从传统面向个人（ToC）消费市场向ToB企业应用转变。5G赋能各行各业，带动行业数字化、智能化转型升级。

5G-Advanced是5G技术的演进版本，其目标是实现万兆体验、千亿物联、智能感知的网络能力。3GPP于2021年12月将R18作为5G-Advanced第一个版本。R18的27个项目涵盖5G传统的eMBB、URLLC、V2X等场景，同时定义了新场景、新业务，如上行大容量、空口人工智能（AI）、虚拟现实增强业务XR、高精度定位等。相比于先前的5G版本，5G-Advanced面向ToB垂直行业应用，在现有网络能力的基础上，进一步提升网络能力，增强支持大上行（1 Gbit/s峰值速率）、极低时延（毫秒级）、更高可靠性（99.9999%）、更高可用性、更高精准授时、更高精度定位，以及通信感知、空天一体的服务保障能力。相应地，5G-Advanced网络的安全技术也要进行增强，以适应在ToB行业的应用推广。

2.1 高可靠性安全

随着5G技术的广泛部署，行业应用普遍对网络可靠性提出确定性要求，如电网差动保护、港口岸桥远程控制、桥式起重机远程操纵等。5G-Advanced的高可靠性增强技术包括PDCP复制、混合自动重传请求（HARQ）重传、智能自适应调制编码（AMC）控制重传和低码率MCS调整等。涉及的安全增强技术主要是PDCP复制安全，即确保PDCP数据和复制数据均使用相同的加密完保策略和密钥，如图2所示。这也是跨站CA和切换场景的密钥一致性解决方案。

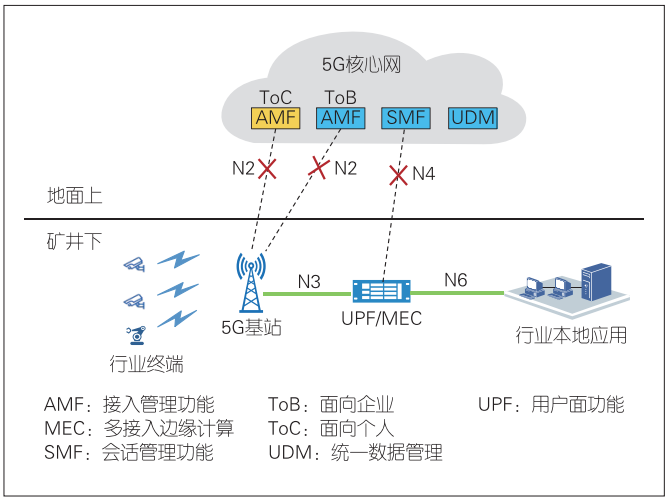


▲图2 基于载波聚合PDCP复制或双连接PDCP复制

2.2 高可用性安全

高可用性是行业应用的基本要求：一方面通过设备和链路冗余提高可用性，例如基站热备支持节点级和网络级的容灾保护，前传光口双上联合环组网，均能保障传输的高可用性；另一方面，要确保在通信链路断开后，仍能继续保持业务连接，例如在矿山场景中，当井下基站和地面核心网链路因事故中断后，基站要支持断链保持功能，使井下用户终端业务不中断。

如图3所示，当矿山场景的井下基站与地面核心网的连接（N2、N4）断链时，为了保持业务连贯运行，井下用户终端的正常业务不受影响，基站需要启动5G控制面（NG-C）断链业务保持功能，并且要求业务不断、安全不断。由于对用户的安全控制管理是在核心网进行的，因此当基站启动断链保持时，基站也要增强对用户的安全控制管理。



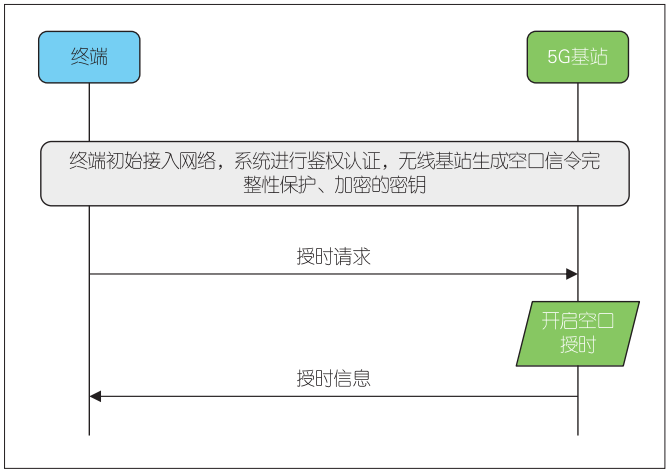
▲图3 5G控制面断链业务保持功能示意

2.3 5G精准授时安全

工业控制、电力差动保护/精密测量单元（PMU）等业务需要严格的业务同步。由于工业控制有线化成本高、布放受限，工业控制网络无线化是一个重点发展方向。特别是随着5G工业互联网产业需求的迅猛发展，5G+垂直行业产业发展迅速，通过5G空口实现业务到UE侧高精度时间同步成为业务系统的基础性需要。5G基站通过空口把网络同步时间传送给UE，同时系统对处理时延进行相应的误差校准，从而实现全网UE的高精度时间同步。

5G空口授时的安全性增强主要是对系统信息模块（SIB）广播消息的增强处理。5G空口授时有两种模式：RRC单播信令、SIB9广播。其中，RRC单播方式拥有空口安全协商接入准入机制，并采用加密的信令对UE进行授时，具有较高的安全性。

图4为5G空口授时的RRC单播方式。基站在发送授时信息时使用安全协商后得到的密钥进行加密和完保，以保证授时信息通过空口传输时的机密性和完整性。



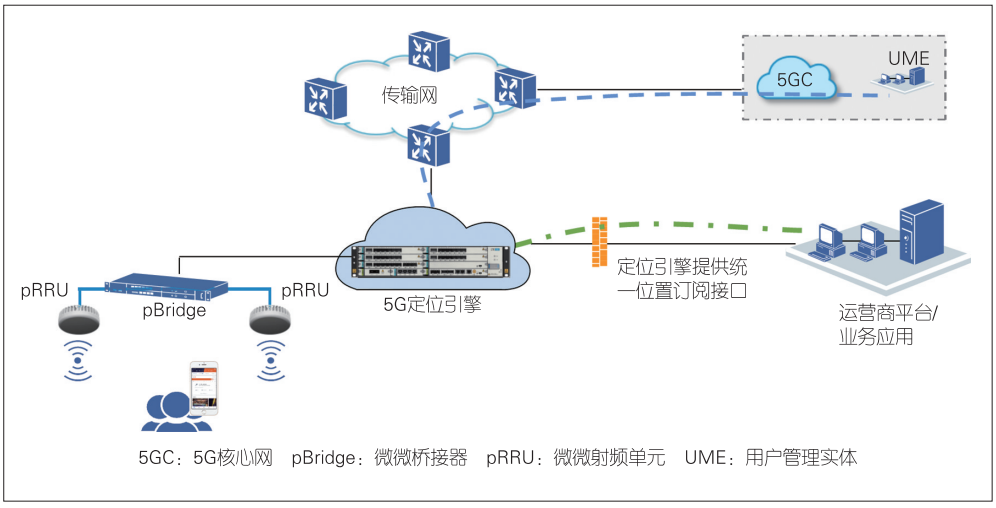
▲图4 5G空口授时的无线资源控制单播方式

而广播方式SIB9消息不需要接入认证就可获取，安全性差，容易受到伪基站攻击。因此，我们需要先考虑增强终端流程安全，确保终端收到的SIB9广播消息的合法性，再重新获取时间信息和使用时钟。

2.4 5G高精度定位安全

位置服务是未来新兴产业的重要驱动力，包括商场、车站、医院的室内导航，移动电子商务、个性化广告的商品引导，救灾抢险的特殊行业人员定位等。传统的卫星定位由于受覆盖和通信能力限制，难以满足未来数字化社会的高精度定位服务需求。5G大规模天线、大带宽的关键技术和算法突破，使得厘米级的高精度定位成为可能，不仅能保障室内室外的无缝覆盖，还具有强大的通信能力。因此，5G高精度定位是未来位置服务的主要手段。

5G空口定位的安全性增强主要是对定位数据的保护，需要严格定义数据访问权限，防止非法访问、防DDOS攻击等。同时位置计算的定位引擎是高精度定位的核心。连接基站、网管和业务平台需要采用不同的网络平面进行隔离，以保证网络安全，如图5所示。



▲图5 5G空口定位结构

2.5 数据分流安全

5G行业应用中数据安全是保障企业开展生产经营活动的重要前提。各类技术资料可能含有重要的商业机密，一旦泄露将导致企业失去核心竞争力。此外，生产控制指令、工况状态等信息若被不法分子篡改，将引发系统设备故障甚至生产安全事故，影响企业生产运行。企业客户普遍提出5G网络的引入需要保证数据不出园的安全需求。

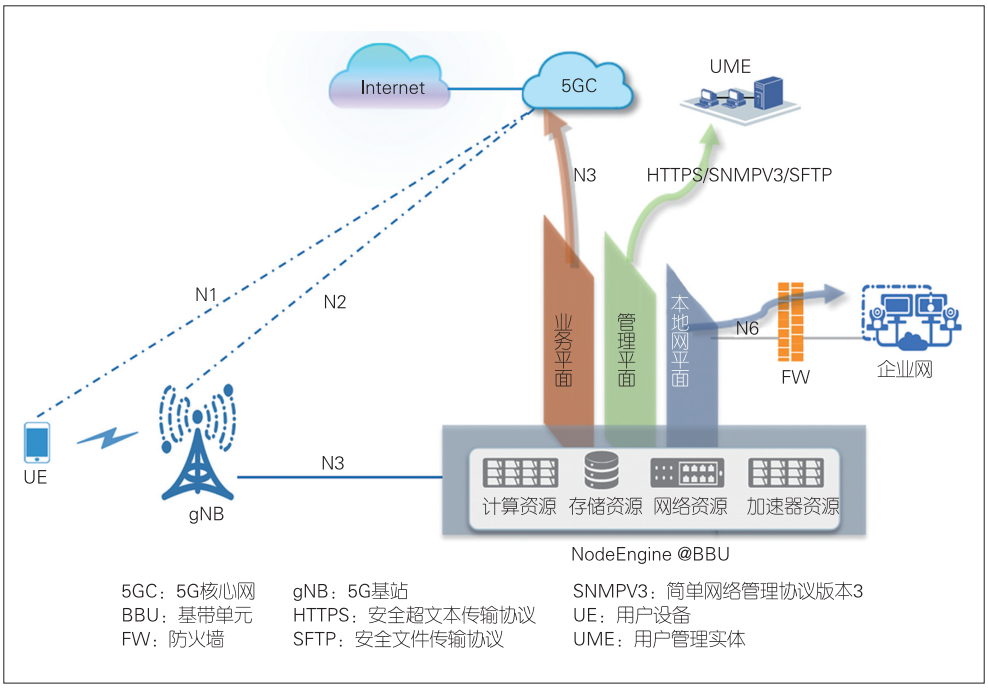
由于ToB业务本地处理需求强烈，我们可通过下沉部署园区专用的本地分流网关来解决数据在本地处理的问题，也可根据业务场景的需要选择基站内置分流功能产品或UPF产品来作为本地分流网关，例如中兴通讯的NodeEngine基站引擎就可实现数据分流，如图6所示。

5G基站集成的数据处理引擎NodeEngine可实现园区业务的本地分流。这不仅使园区业务就近得到处理，提高业务处理的实时性，还可满足园区业务不出园的安全需求。NodeEngine可以根据业务部署的需要灵活支持IP五元组/域名服务器（DNS）域名、切片标识以及公共陆地移动网络（PLMN）的数据分流机制。

NodeEngine采用虚拟本地网（VLAN）隔离和隐藏UE IP等安全隔离措施，满足智简园区的组网安全。NodeEngine在对接基站、网管、企业专网时采用不同的网络平面，各网络平面采用VLAN隔离，以保证网络安全；在企业专网内部UE IP与运营商传输网络IP不同的情况下，支持对专网UE IP进行网络地址转换（NAT），以对外隐藏UE IP。

3 6G内生安全

6G网络设计将在很多方面和5G有着显著的不同。首先，6G可以实现网络自动化和网络即服务（NaaS），用户可



▲图6 5G行业应用数据分流示意图

以定制网络；其次，核心/无线网络组件的云化网络和开源软件的快速应用表明，未来6G将是“完全开放”的网络。因此，6G安全架构需要适应变化，支持新的应用和太空-空中-地面-海洋网络模型的集成[4]。中国的6G相关科研工作启动比较早。2019年6月工业和信息化部牵头成立中国IMT-2030（6G）推进组，标志着中国6G研发正式启动。IMT-2030（6G）推进组认为：6G将实现人与人、人与物、物与物的高效智能互联，打造泛在精细、实时可信、有机整合的数字世界，实时精确地反映和预测物理世界的真实状态，助力人类走进人机物智慧互联、虚拟与现实深度融合的全新时代，最终实现“万物智联、数字孪生”的美好愿景[5]。在6G给社会经济生活带来变革的同时，安全性显得至关重要。网络安全技术需要实现颠覆性的突破。传统“外挂式”、“补丁式”的安全机制将向内生安全演进。

IMT-2030（6G）推进组把内生安全列为6G潜在的十大关键技术之一，同时定义网络内生安全的四大特征：（1）主动免疫，为网络基础设施、软件等提供主动防御功能；（2）弹性自治，实现安全能力的动态编排和弹性部署；（3）虚拟共生，实现物理网络与虚拟网络安全的统一与进化；（4）泛在协同，通过端、边、网、云的智能协同来准确感知整个网络的安全态势[6]。本文中我们认为，轻量化也是6G内生安全的主要特征之一，而传统的接入安全技术无法满足海量设备连接和实时传输，需要有轻量化的安全机制来满足6G万物智联、数字孪生的应用场景需求。

3.1 主动免疫

网络安全攻击的目的与攻击手段在不断变化，所以安全的风险也会持续不断变化。与传统5G安全被动式地应对安全攻击和风险不同，6G内生安全提供了一种主动免疫的解决思想，赋予网络以类似人体免疫的安全能力。因此，内生安全也被称为新的网络安全范式。

（1）AI/机器学习（ML）安全

AI/ML将全方位赋能6G网络安全。基于AI/ML的安全内生机制使得6G网络具备主动免疫、自我演进、按需提供安全服务的能力。具体来说，使用深度强化学习和深度神经网络进行入侵检测和预防，可以有效防御网络中的伪基站攻击、IP欺骗攻击、DDoS攻击、控制平面饱和攻击和主机位置劫持攻击等；使用AI预测分析可以在攻击发生之前预测攻击，例如基于强化学习（RL）的智能波束成形技术可提供针对6G太赫兹和可见光通信系统中窃听者攻击的最佳波束成形策略；基于边缘的联邦学习能够在6G分布式网络的海量设备和数据机制中执行网络安全任务。

未来基于AI/ML的主动免疫内生安全演进过程分为3个阶段。（a）初级阶段：基于AI/ML、威胁模型、关联分析模型等，按规划进行安全能力建设，初步形成免疫能力；（b）中级阶段：进一步基于AI/ML和网络空间灾害模型等提升网络免疫能力，仅需要部分人工干预，使网络安全建设具备一定的可控和收敛能力；（c）高级阶段：网络的主动免疫能力能够量化，安全能够弹性自治，基本不再需要人为干预[7]。

（2）区块链技术

区块链是一种以密码学算法为基础的分布式账本技术，可在去中心和多中心的系统中实现不可篡改和防伪，并保证各个节点账本的动态一致性，其本质是一种互联网共享数据库，具有主动免疫特性，能够帮助6G网络构建安全可信的通信环境。区块链在中国受到高度重视。2021年中国的“十四五”规划明确提出：区块链是新兴数字产业之一，需要“以联盟链为重点发展区块链服务平台和金融科技、供应链管理、政务服务等领域应用方案”。可以预见，区块链将是6G时代数字化经济形态所覆盖的数千万甚至数以亿计的资

产单位或机器（物联网）的分布式、安全交易模式，并有望成为6G网络内生安全的关键技术。文献[8]研究了区块链技术与6G频谱管理融合发展（特别是共识机制、合约机制技术）的深入应用，有效提高频谱利用率，实现动态、高效的频谱资源管理，为6G网络营造一个安全、智能、可行的动态频谱共享环境。文献[9]面向6G零信任网络的通信需求，以区块链为“信任桥梁”，研究了6G车联网边缘计算中的可信可靠接入管理方法。该方法在不泄露车辆隐私的前提下显著提升了车辆验证效率，降低了基站能耗，具有更高的安全性。

6G时代的mMTC场景将实现去中心化转变，以支持海量设备连接。这和区块链的去中心化特征非常适配。区块链具有不可篡改、全程留痕、可追溯、集体维护、公开透明等特点，可以很好地满足内生安全设计需求，是6G内生安全的候选关键技术。区块链可能是最具颠覆性的万物互联技术之一[10]。当然，区块链要成为6G内生安全技术，需要关注自身部署形态，尤其是在工业物联网等ToB行业应用中，区块链+边缘计算的部署形态，以保障链上链下数据的可信交互；还需要关注高可靠低时延的区块链链上链下通信方式，以支持在多类型终端大数据容量和复杂网络环境下数据的高效安全传输，以及区块链系统与其他系统之间的数据交换。

3.2 弹性自治

6G网络的行业应用场景，例如增强现实（AR）、虚拟现实（VR）等，对网络时延、传输速率、连接数等需求差异巨大。传统5G网络受限于网络架构、交付方式、运维模式等，难以满足不同行业的应用需求。因此，6G网络安全应具备内生弹性可伸缩的框架。基础设施应具备安全服务灵活拆分与组合的能力，通过软件定义安全、虚拟化等技术，构建随需取用、灵活高效的安全能力资源池，实现安全能力的按需定制、动态部署和弹性伸缩，适应云化网络的安全需求。

文献[11]设计了一种6G网络内生安全架构。该架构包括安全管理中心、安全智能中心、安全策略控制单元、安全能力层（网元设备自身安全能力、专用安全能力资源池）4层，并结合信任共识设施、资源编排与调度能力、人工智能分析能力，形成体系化安全架构，如图7所示。

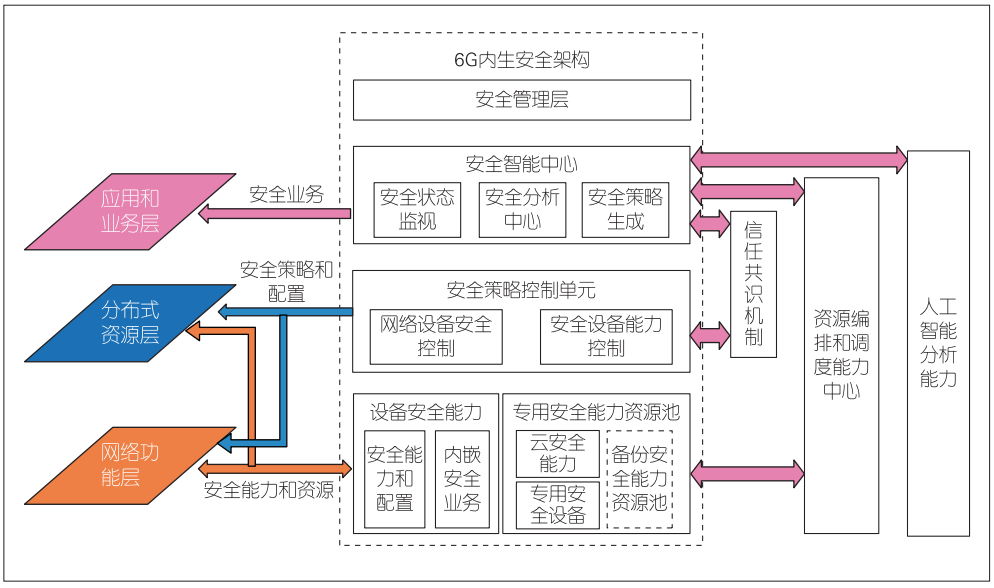
在图7所示的6G内生安全架构中，设备安全能力可保障设备基础安全功能应由设备自身提供，还可有效保障设备在其他安全机制失效时仍能维持基本的安全能力；专用安全能力资源池提供实现共性安全能力，其目标是保障安全能力高效执行，避免系统中安全能力的重复建设与部署；安全策略控制单元执行安全智能中心的安全策略下发，包括网元设备的安全策略、安全专用设备的安全策略；安全智能中心是安全协同的大脑，基于AI能力，与管理中心、资源编排与调度能力联动；安全管理中心提供系统管理、审计管理、安全管理、集中管控等能力，并能呈现安全态势等。

在安全管理中心的指导下，以6G网络安全能力为基础，配合柔性安全能力资源池，协同智能分析与编排机制，可构建弹性自治的安全防护体系。这样的体系具备对外安全服务能力，能够达到主动免疫、信任共识、协同弹性的目标。

3.3 虚拟共生

相比于传统5G网络，6G网络将打通物理世界和虚拟世界，形成物理网络与虚拟网络相结合的数字孪生网络，在工业控制、体育场馆、新闻媒体、社交娱乐等领域有着广泛的应用前景。XR技术利用硬件设备并结合多种技术手段，将虚拟的内容和真实场景融合，通过计算机技术和可穿戴设备产生一个真实与虚拟组合的、可人机交互的环境，包括VR、AR、混合现实（MR）等多种形式，不仅可以实现数字和物理世界的社交属性的充分放大，还可基于共同的物理空间和虚拟空间分享信息。

个人数据的管理是XR应用必须考虑的安全要素。通过



▲图7 6G内生安全参考架构

6G网络进行的数据收集、存储、保护和共享必须遵守相应的数据保护规范和条例。文献[12]认为超低时延网络的可靠性是解决网络动态的关键，同时发现一些网络攻击过于复杂、无法防御，因此敏感和机密数据仍可以被公开。为此，文献[13]提出一种高效的物理层安全技术——正交频分复用（OFDM）及子载波索引选择，通过开发联合优化子载波索引选择（IS）和自适应交织（AI）设计，最大限度地提高仅在合法接收机处的信噪比，来保护基于OFDM的波形在无线网络之外免遭窃听。该技术适用于URLLC场景的安全保护。

文献[14]提出一个3D系统，针对许多XR系统的隐私数据威胁进行风险建模。另外，文献[15]提出一种基于Delta正交多址接入（D-OMA）的物理层安全方案。该方案可增强上下行无线接入网的安全性，能够应用于XR的安全解决方案，扩展6G XR设备的访问能力，如图8所示。

D-OMA的安全方案是基于拼图概念实现的。在上行链路中，每个XR设备都有代表最终簇密钥（CK）的特定部分密钥（PK）。在接收端，将来自同一群集中不同XR设备的PK部分组合，可最终形成完整的CK。这与多因素并行身份验证过程类似。组合CK被视为所有设备从该集群中接收的数据的解密密钥。在未完全确认该密钥的情况下，系统将不会重构来自所有设备的数据。也就是说，窃听器需要以相同的时间和顺序解码所有用户的数据。而当大量XR终端设备传输到单一上行链路接收器时，这是比较难以实现的。只有接收基站知道运行期间所需的解码顺序以及每个XR群集的内容，从而确保XR设备的数据安全。

3.4 泛在协同

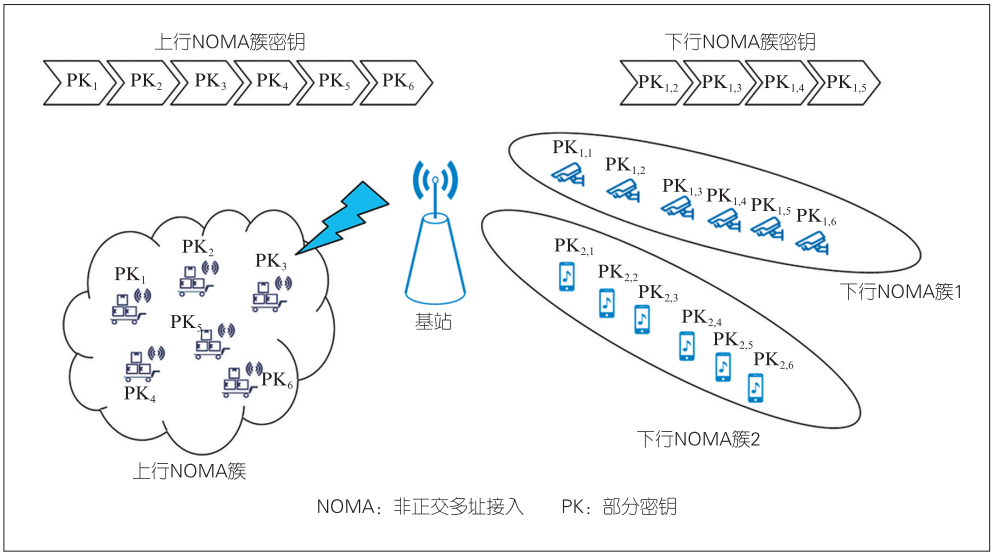
6G时代网络赋能各行各业，将传统封闭的通信技术（CT）领域融入信息技术（IT）领域。在这个变革的过程中我们可以发现，不同于传统5G通信网络的特性，6G网络更多地面对ToB领域。在确保有足够的专业维护手段来保障网络核心效果的同时，面对千行百业存在的特异性差别，行业间的技术壁垒和巨大的学习成本衍生出对端、边、网、云泛在协同的智能运维的诉求。各行业在安全生产、传输高可靠性、生产长连接保障、网络建设成本控制等方面存在刚性需求。在智慧内生的6G网络中，ML和大数据分析技术在安全方面将得到广泛应用。在AI技术的赋能下，6G网络能够建立端、边、网、云智能主体间的泛在交互和协同机制，准确感知网络安全态势并预测潜在风险，进而通过智能共识决策机制完成自主优化演进，实现主动纵深安全防御和安全风险自动处置[6]。

例如，中兴通讯的智能数字化运维服务系统（iDOS），通过关联端侧、无线、传输等各域数据，以业务精准识别端到端体验建模为核心，运用AI数据挖掘算法，实现对企业网络和业务指标的异常识别、故障的业务详单和信令级回溯、端到端问题定界，关联同时间、同维度、同域数据分析，进行故障的最终定位，协助客户监控业务整体运行状况、定位故障，从而提升对整个网络的运维支撑能力[16]，如图9所示。

iDOS从运维出发，提供智能化安全态势感知和主动故障预防机制，通过AI引擎持续在线进行ML和迭代更新，训练生成网络健康度量模型，并应用于实时的设备和网络健康监控，快速发现可能导致业务质量下降的网络风险、设备故障、外部环境风险等，提供最佳处理建议，真正做到防患于未然。通过长期监控数据，iDOS可提前识别设备、链路和环境等网络平稳运行的影响因素，对健康度进行评估，精准识别潜在的风险并预测故障发生的时间，在故障发生之前提示用户。此外，iDOS还可通过主动预防，提前识别并更换存在隐患的硬件，指导运维人员针对环境风险进行整改，从而极大降低网络故障发生率，确保企业业务所需要的高可靠性[16]，如图10所示。

3.5 轻量化

未来6G应用场景的通信技术将从人的通信转变为物的



▲图8 基于Delta正交多址接入提供的安全方法

通信、以下行为主转变为上行为主、以基站为中心转变为去中心化。传统的接入技术无法满足物理网等海量设备接入和实时传输，会引发网络拥塞问题。另外，mMTC场景在满足物联网、工业现场网络、智慧城市等应用同时，也会面临网络安全挑战，例如在终端、接入和数据方面的安全威胁：

（1）终端安全威胁。mMTC场景下的终端具有低功耗、低成本的特点，但海量终端的计算资源和存储资源有限，难以支持复杂的安全防护机制和强安全加密算法，因此安全防护能力较弱，容易成为攻击者的主要目标。

（2）接入安全威胁。mMTC场景下的设备数量庞大，海量的终端设备接入网络后同时触发接入认证流程，容易引起信令风暴，导致网络拥塞并加大终端设备的能源消耗。因此，针对这类设备的认证机制需要进行简化。采用高效而轻量化的认证机制，可减少认证时间，减轻网络拥塞程度。

（3）数据安全威胁。在mMTC业务场景中，网络服务、功能及数据的开放共享增加了对用户隐私和敏感数据的完整性和机密性保护难度。如未采取必要的数据保护措施，则可能会引发数据泄露风险。采取用户权限管理、安全认证、安全隔离、网络安全加固、审计等措施，可有效提升数据安全能力。

因此，传统5G接入技术无法满足mMTC场景海量设备连接和实时传输需求，需要演进为轻量化的接入和认证技术，实现极简无连接和高过载传输的海量设备互联。例如，多用户共享接入（MUSA）技术就实现了简化传输交互流程和去中心化，以支持海量设备互联。经过实测，MUSA可实现每平方公里9 000万次的连接，这是国际电信联盟（ITU）定义的90倍。相应的安全保护机制也是mMTC场景的安全关键技术，具体可从轻量级接入认证、轻量级密钥管理及加解密、隐私数据保护等来寻求安全解决方案。

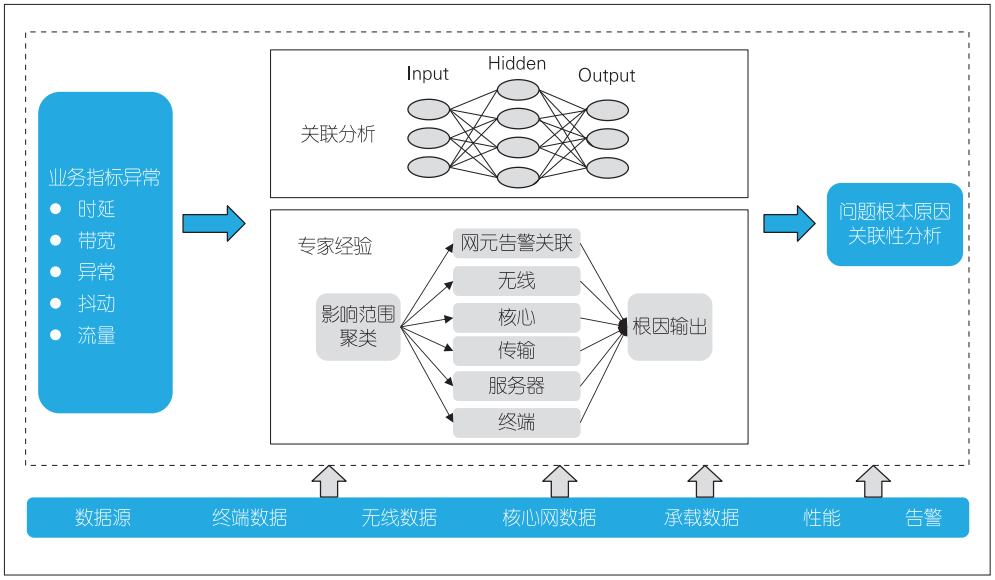
（1）轻量级接入认证

针对mMTC场景的MUSA技术简化了接入信令交互流程，有时甚至只需要1条信令就能实现用户接入，因此有必要建立支持大规模设备的、灵活可靠的认证机制。简化算法和运算逻辑，完成海量设备和网络侧的认证，既能保证连接的安全性，又能降低对资源的使用。

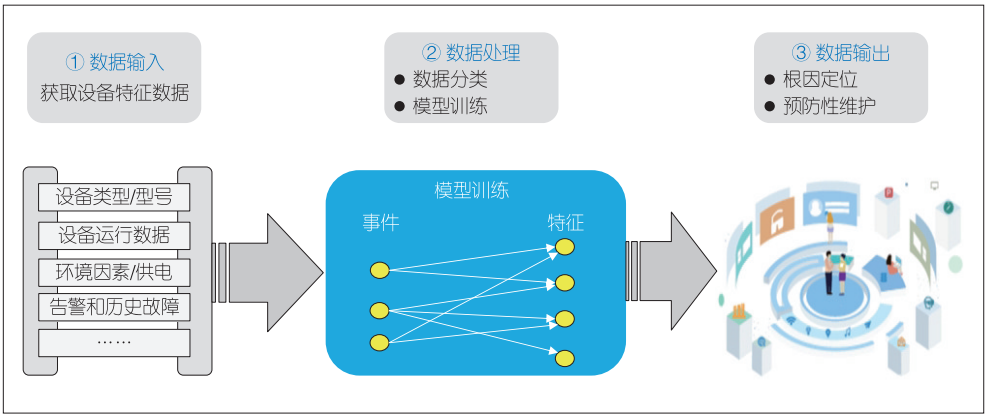
物理层认证是实现轻量级接入认证的关键技术之一。利用无线网络物理层的私有信道特征实现的低复杂度、高安全性的安全方案，分为基于设备指纹的认证和基于信道指纹的认证两种。前者利用硬件设备的电特性差异提取设备独有的特征，将唯一标识作为设备的认证指纹；后者不需要额外的信号提取设备，从无线信道特征入手，利用不同位置设备的信道特征之间存在的不相干性进行认证。文献[17]提出一种在认证过程中可以使用的非监督式学习方法，来增强物理层的安全性。

（2）轻量级密钥管理及加解密

传统密码学技术的核心是依靠密钥强度来保护系统安



▲图9 泛在协同智能运维系统



▲图10 人工智能赋能安全态势感知

全，使得攻击者在有限的时间和算力条件下无法破解密钥。而海量终端设备由于能力受限，无法提供复杂的密钥管理和密钥存储条件，导致传统密码学技术难以使用，因此需要引入轻量级的密钥管理和加解密技术。

物理层密钥生成技术也是实现轻量级密钥管理和加解密的解决方案。其原理是利用发射和接收信道中的随机熵来生成用于通信的保密密钥[18]。通过信道的互易性、时变性、唯一性等特征，基站与用户对信道进行探测，得到共同随机性以生成对称密钥，进行轻量级的加解密处理。物理层密钥生成可以做到一次一密（OTP），实现最强的密码安全保护。

（3）隐私数据保护

终端数据传输保护技术包括空口加密和完整性保护、非接入层（NAS）信令加密和完整性保护、无线资源控制（RRC）信令加密和完整性保护、空口业务数据加密和完整性保护等。在mMTC场景中，诸如自动驾驶、可穿戴设备、远程医疗终端等物联网设备在日常使用中会收集、存储和传输大量个人隐私数据。个人数据可以是与已识别或可识别人员直接或间接相关的任何信息，如姓名、身份证号码、用户位置和社交身份[19]。我们需要根据不同的业务场景和用户对象提供差异化的隐私数据保护能力，对用户隐私数据的请求、存储、传输等各个环节采取隐私保护措施。

4 结束语

在5G之前，甚至在5G-Advanced阶段，安全技术都不是内生的，而是对业务功能的补充和增强。随着6G颠覆性技术应用（如太赫兹和可见光通信、智能表面技术、通信感知一体化等）的发展，6G网络架构和形态将发生系统性变化。网络安全不再是传统的“外挂式”和“补丁式”，而是内生的。这也是人们进行6G安全研究的共识。

本文中，我们回顾了5G的基础安全能力和技术，以及5G-Advanced的安全技术演进，并分析了6G内生安全特征和内生安全关键技术，希望为后续6G安全技术研究提供参考。

参考文献

[1] 3GPP. Security architecture and procedures for 5G system (release 15): 3GPP TS 33.501 [S]. 2019

[2] 陆海涛, 李刚, 高旭昇. 5G网络的设备及其 接入安全 [J]. 中兴通讯技术, 2019, 25(4): 19-24+55. DOI: 10.12142/ZTETJ.201904004

[3] 聂凯君, 曹傧, 彭木根. 6G内生安全：区块链技术 [J]. 电信科学, 2020, 36(1): 21-27

[4] ABDEL HAKEEM S A, HUSSEIN H H, KIM H. Security requirements and challenges of 6G technologies and applications [J]. Sensors, 2022, 22(5): 1969. DOI: 10.3390/s22051969

[5] IMT-2030(6G)推进组. 6G总体愿景与潜在关键技术白皮书 [R]. 2021

[6] IMT-2030(6G)推进组. 6G网络安全愿景技术研究报告 [R]. 2021

[7] 中兴通讯. 2030+网络内生安全愿景白皮书 [R]. 2021

[8] 牛娇红, 黄何, 王卫斌, 等. 区块链技术及其6G网络中应用探析 [J]. 信息通信, 2020, 33(11): 37-39

[9] 郝敏, 叶东东, 余荣, 等. 区块链赋能的6G零信任车联网可信接入方案 [J]. 电子与信息学报, 2022, 44(9): 3004-3013

[10] SAAD W, BENNIS M, CHEN M Z. A vision of 6G wireless systems: applications, trends, technologies, and open research problems [J]. IEEE network, 2020, 34(3): 134-142. DOI: 10.1109/MNET.001.1900287

[11] 粟栗, 庄小君, 杜海涛, 等. 6G网络内生安全架构研究. 中国科学: 信息科学, 2022, 52(2): 12. DOI: 10.1360/SSI-2021-0257

[12] CHEN R Q, LI C H, YAN S H, et al. Physical layer security for ultra-reliable and low-latency communications [J]. IEEE wireless communications, 2019, 26(5): 6-11. DOI: 10.1109/MWC.001.1900051

[13] HAMAMREH J M, BASAR E, ARSLAN H. OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services [J]. IEEE access, 2017, 5: 25863-25875. DOI: 10.1109/ACCESS.2017.2768558

[14] YAMAKAMI T. A privacy threat model in XR applications [M]//Advances in Internet, Data and Web Technologies. Cham: Springer International Publishing, 2020: 384-394. DOI: 10.1007/978-3-030-39746-3_40

[15] AL-ERYANI Y, HOSSAIN E. The D-OMA method for massive multiple access in 6G: performance, security, and challenges [J]. IEEE vehicular technology magazine, 2019, 14(3): 92-99. DOI: 10.1109/MVT.2019.2919279

[16] 中兴通讯. ToBeEasy极简运维技术白皮书 [R]. 2021

[17] SATTIRAJU R, WEINAND A, SCHOTTEN H D. AI-assisted PHY technologies for 6G and beyond wireless networks [EB/OL]. [2022-10-16]. https://arxiv.org/abs/1908.09523

[18] TANG J, JIAO L, ZENG K, et al. Physical layer secure MIMO communications against eavesdroppers with arbitrary number of antennas [J]. IEEE transactions on information forensics and security, 2021, 16: 466-481. DOI: 10.1109/tifs.2020.3015548

[19] European-Union. General data protection regulation [R]. 2016

作 者 简 介

陆海涛，中兴通讯股份有限公司5G研发安全总监，高级工程师，CISSP；主要从事无线网络架构、无线产品安全、大规模天线、动态频谱共享等技术研究；牵头和参与10多项国家科技重大专项、“863”计划课题，获广东省科技进步奖；发表论文8篇，申请发明专利60多项。

陈一喆，南京邮电大学在读本科生；研究方向为物联网、网络安全、机器视觉、深度学习等；参与多个科研项目，其中两个项目分别获得“互联网+竞赛”江苏省一等奖和“双创大赛”江苏省二等奖。

娄笃仕（通信作者），中兴通讯股份有限公司5G研发总工、高级工程师；主要从事CDMA/WiMAX/LTE/5G移动通信技术方面的研究工作；拥有丰富的无线系统产品设计和研发经验，牵头中兴通讯5G基站产品总体方案设计和研发管理；申请发明专利15项，发表论文多篇。