AI赋能6G网络安全：架构与关键技术

AI Empowered 6G Security: Architecture and Key Technologies

王瀚洲/WANG Hanzhou，金子安/JIN Zian，
王瑞/WANG Rui，刘建伟/LIU Jianwei
（北京航空航天大学，中国 北京 100191）
(Beihang University, Beijing 100191, China)

DOI：10.12142/ZTETJ.202503006
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20250606.1502.002.html
网络出版日期：2025-06-09
收稿日期：2025-04-15

摘要：针对6G网络架构中的需求与挑战，探讨了“主动免疫-孪生互驱-弹性自治-分布协同”的智慧内生安全架构。该架构通过预训练威胁表征模型实现攻击前预判，利用数字孪生构建虚实结合防御体系，借助联邦学习与区块链技术建立跨域协同机制，形成“感知-决策-验证-优化”的安全闭环。介绍了5项6G网络安全中的关键技术：分布式机器学习、AI大模型、轻量级认证授权与访问控制、数字孪生、无线物理层安全技术，为6G网络的高效可信运行提供理论支撑与技术路径分析。

关键词：6G网络安全；人工智能；分布式机器学习；大模型；轻量级认证授权与访问控制；数字孪生；无线物理层安全

Abstract: In response to the requirements and challenges of the 6G network architecture, an intelligent endogenous security architecture of “proactive immunity, twin-driven, resilient autonomy, and distributed collaboration” is proposed. This architecture enables proactive threat prediction through pre-trained threat representation models, constructs a cyber-physical integrated defense system using digital twins, and leverages federated learning and blockchain technologies to facilitate cross-domain collaboration, forming a security closed loop of “perception, decision, verification, and optimization.” Five key technologies for 6G network security are introduced: distributed machine learning, AI large models, lightweight authentication and access control, digital twins, and wireless physical layer security technologies. These technologies provide theoretical support and technical pathways for the efficient and trustworthy operation of 6G networks.

Keywords: 6G security; artificial intelligence; distributed machine learning; large model; lightweight authentication authorization and access control; digital twin; wireless physical layer security

引用格式：王瀚洲，金子安，王瑞，等. AI赋能6G网络安全：架构与关键技术 [J]. 中兴通讯技术，2025，31(3)：31-39. DOI：10.12142/ZTETJ.202503006
Citation: WANG H Z, JIN Z A, WANG R, et al. AI empowered 6G security: architecture and key technologies [J]. ZTE technology journal, 2025, 31(3): 31-39. DOI: 10.12142/ZTETJ.202503006

1 6G网络安全需求

6G网络从逻辑角度可初步划分为3个层次：基础设施与物理层、网络连接与功能层、能力开放与服务层。各层级在安全方面呈现出高可靠、泛融合、强隐私等显著区别于5G网络的特征[1]。本文从6G网络的分层安全需求出发，探讨基于闭环控制思想的内生安全架构设计，以应对6G网络所面临的安全挑战。

1.1 能力开放与服务层

6G网络能力开放与服务层为用户提供多样化服务与应用接口，其核心安全目标在于实现数据、访问实体及应用服务的智能治理，主要体现在以下3个方面：

1）数据安全与隐私保护。6G网络的沉浸式通信、通信感知一体化等业务场景涉及大量用户敏感信息，包括生物特征、行为数据、位置信息及个人习惯等。需保障数据在传输、存储和处理全生命周期的保密性、完整性和可用性，防止未授权访问、窃取及篡改。

2）访问控制与认证授权。6G网络的泛在连接特性导致不同组织的通信设备与服务应用共存，因此要构建安全可靠

基金项目：国家重点研发计划项目（2021YFB2700200）；国家自然科学基金项目（U21B2021，61972018，61932014）

的信任关系。另外，还需建立轻量级分布式访问控制与认证授权机制，支持多模态认证方式，实现多因素联合鉴权，确保仅授权实体可访问相应资源与服务。

3）新兴技术与服务安全。在人工智能、区块链等新兴技术与通信网络深度融合的背景下，6G网络需重点保障AI模型的抗攻击鲁棒性，通过实时更新机制适应动态网络环境，并增强模型可解释性。针对新兴技术衍生的动态服务，需建立实时运行监测体系，实施微隔离防护策略，确保在快速迭代与灵活部署过程中实现安全策略的无缝衔接与持续有效性。

1.2 网络功能与连接层

6G网络功能与连接层负责网络资源调度、连接管理和数据传输等功能，其核心安全目标在于实现分布式网络的安全跨域协同，主要体现在以下3个方面：

1）切片安全隔离。6G网络切片需采用切片安全隔离技术，在硬件层面，需基于新型网络接口卡实现物理隔离；在软件层面，依托网络功能虚拟化技术实现逻辑隔离。同时，结合数字孪生技术实时仿真切片内威胁演化，动态调整隔离策略，有效阻断攻击跨切片扩散。

2）控制面可信协同。6G网络控制面采用分布式控制架构（如软件定义网络控制器集群）实现网络功能调度与策略管理。通过区块链与智能合约技术确保控制节点间的可信协作，防止恶意节点策略注入，利用强化学习等技术持续优化控制面策略，提升网络运行效率。

3）边缘网络轻量化防护。面向资源受限的边缘6G网络环境，需构建轻量化安全防护体系。通过部署轻量级AI模型，基于设备行为模式识别等动态信任评估方法，实现接入权限与资源分配的动态调整。同时，支持本地化快速威胁检测与响应，包括恶意设备识别、异常流量过滤等功能，在保障安全性的同时满足边缘计算对低时延的严格要求。

1.3 基础设施与物理层

6G网络基础设施层由超密集异构节点构成，涵盖边缘计算节点、太赫兹基站及卫星基站等多样化设备，其核心安全目标在于保障海量硬件节点的可信运行。值得注意的是，随着智能超表面（RIS）等物理层技术的突破，基础设施层已具备承载部分网络连接层安全功能的能力，具体体现在以下3个方面：

1）硬件可信安全增强机制。采用物理不可克隆函数（PUF）实现设备身份唯一性标识，结合可信执行环境（TEE）构建硬件级安全防护体系。该机制可有效确保设备身份不被伪造、防御固件层恶意篡改，阻断硬件注入攻击，为上层网络连接与数据处理功能提供可信硬件运行环境。

2）物理层信号传输安全。6G网络通过RIS与自适应波束成形技术，实现信号能量在目标接收方向的空间聚焦，显著提升物理层信号的抗干扰能力。

3）承载密钥生成能力。利用物理信号与信道的随机性特性生成密钥进行加密，为数据传输提供额外的安全保障。

2 AI赋能6G网络安全架构

AI技术与通信网络安全的深度融合始于5G时代，它推动网络安全架构从被动防御向主动防御演进。基于AI的决策算法与模型验证技术被广泛应用于网络安全领域，典型研究包括：L. CAVIGLIONE等通过神经网络与决策树构建检测模型，以设备能耗为特征，识别移动恶意软件利用合谋应用建立的隐蔽通信通道[2]；M. BOTHA等将模糊逻辑神经网络与趋势分析相结合，构造主动动态检测模型，以减少和控制计算机系统中的入侵行为[3]；蔡良伟等基于正态自适应遗传优化算法改进深度包检测方案，使正则表达式匹配的空间复杂度降低，可更好地发掘并控制应用层中的恶意流量[4]。这些研究表明，AI技术在安全策略部署、入侵检测等自动化决策任务中展现出显著优势，增强了传统安全机制的稳定性、灵活性和实时响应能力。然而，5G时代的AI应用主要集中于安全功能增强层面，与网络架构的深度集成不足，尚未实现安全能力与网络架构的有机融合，缺乏系统化的内生安全智能体系。

在6G时代，通信网络呈现定制化、异构化和开放化的发展趋势，网络规模与复杂度显著提升，超低时延与超大带宽特性要求实时防护能力，个性化服务则加剧隐私保护难度。为应对以上安全挑战，亟需通过具备自感知、自决策、自学习能力的人工智能技术，构建体系化、一体化的内生安全架构。

随着通信技术从5G向6G演进，网络安全架构通过AI技术在网络各层次的不断深化，正逐步实现真正意义上的内生安全体系。基于文献[5]提出的6G网络内生安全框架，本研究构建了以人工智能为核心的分布式智能内生安全架构，其核心特征主要体现在以下4个方面。

1） 主动免疫

基于多模态数据（包括流量特征、协议解析及物理层信号）的预训练威胁表征模型，融合在线学习机制实时捕获零日攻击特征，动态生成路由调整、虚拟补丁等防御策略，构建网络对未知威胁的主动免疫能力。该机制通过攻击前预判实现动态防御，例如采用扩散模型模拟高级持续性威胁（APT）攻击路径并实施预加固。相较于传统基于规则匹配的

被动防御，该方案在检测与响应环节引入学习与预测机制，推动安全防护范式从“特征匹配”向“威胁推演”演进。

2） 孪生互驱

网络孪生体采用强化学习算法在虚拟环境中预演各类攻击场景，生成防御策略并验证有效性后，将其同步至物理网络；信道状态信息、设备能耗等实时参数以极低时延同步至孪生模型，以提升仿真精度。典型应用包括基于孪生体提前模拟信道干扰攻击场景、制定训练抗干扰波束赋形策略。相较于传统依赖静态测试用例验证安全能力的静态开环方案，孪生互驱通过高保真仿真与在线反馈，实现防御策略的低成本迭代，构建从虚拟推演到物理执行循环的安全闭环协同体系。

3） 弹性自治

基于软件定义安全及网络功能虚拟化技术，传统基于专用硬件的安全功能（如防火墙、入侵检测系统等）被解耦为可编程的虚拟安全功能组件，实现按需定制与动态部署。基于意图网络实时感知业务需求与威胁态势，自动拆分、组合异构安全资源，实现安全策略的弹性伸缩与无缝迁移。例如，在分布式拒绝服务（DDoS）攻击突发时，快速调度边缘计算资源部署流量清洗服务，在攻击结束后自动释放。相较于传统安全资源固定配置，弹性自治实现安全资源的动态编排与按需供给，适配6G网络高动态、多场景的业务需求，同时优化资源利用率与成本效益。

4） 分布协同

基于区块链与联邦学习实现跨域节点间的可信协作，消除对中心化信任锚点的依赖。节点间借助智能合约共享威胁情报，并参与联邦模型训练以提升全局检测精度；利用门限签名技术等达成分布式共识，即便部分节点遭劫持，依然能够保障决策的可靠性。例如，在多运营商联合检测跨境APT攻击场景中，通过联邦学习实现模型聚合，达成联合安全威胁检测。相较于传统中心化安全运维模式，群体共识通过分布式智能架构抵抗单点失效风险，并借助群体博弈机制有效抵御女巫攻击与合谋作恶行为。

6G网络基于以上4项特征，分别实现了威胁感知决策、策略推演验证、资源弹性调度、效能评估优化。该逻辑闭环的4阶段协同作用，形成了6G网络内生安全架构，其示意图与各阶段典型安全能力如图1所示。

3 6G网络安全关键技术

3.1 分布式机器学习

随着通信网络的演进建设，6G网络基础设施呈现明显的分布式架构，数据分布于数百亿量级的海量设备。当前，更庞大复杂的智能学习模型往往无法由单一计算节点承载．将数据留存本地进行分布式训练，仅传输特定数据特征而非原始数据流的分布式学习模式，成为实现极低时延模型更新与应对数据隐私问题的解决方案。从安全角度考虑，6G网络泛在连接特性致使攻击面扩大化、分散化，且网络威胁在人工智能技术赋能下，呈现攻击范围扩大、跨域隐蔽性增强与防御实时性需求激增的特征。分布式机器学习突破传统集中式架构“数据向中心汇聚”的底层逻辑，借助群体学习算法实现分布式节点自治与全局协同，有效消除数据传输延迟及中心节点决策延迟[6]；通过多智能体强化学习算法完成环境感知与多视角动态博弈，解决防御策略碎片化问题[7]；通过联邦学习算法达成“数据不动模型动”，防范数据跨域流动引发的隐私泄露风险，进而助力6G网络提升威胁响应效率、完善防御策略体系并增强数据隐私保护[8]。分布式机器学习的算法范式详见表1。将上述3种算法与区块链、安全多方计算等技术深度融合，能够有力推动6G网络安全从“集中式静态防御”向“分布式协同防御”转型升级。

6G网络分布式基础设施与人工智能技术的深度融合，催生出基于分布式机器学习的协同防御体系。该体系凭借横向协同、纵向协同、隐私协同三重机制，突破传统集中式防御的单点瓶颈，其实现路径可分解为以下3个方面：

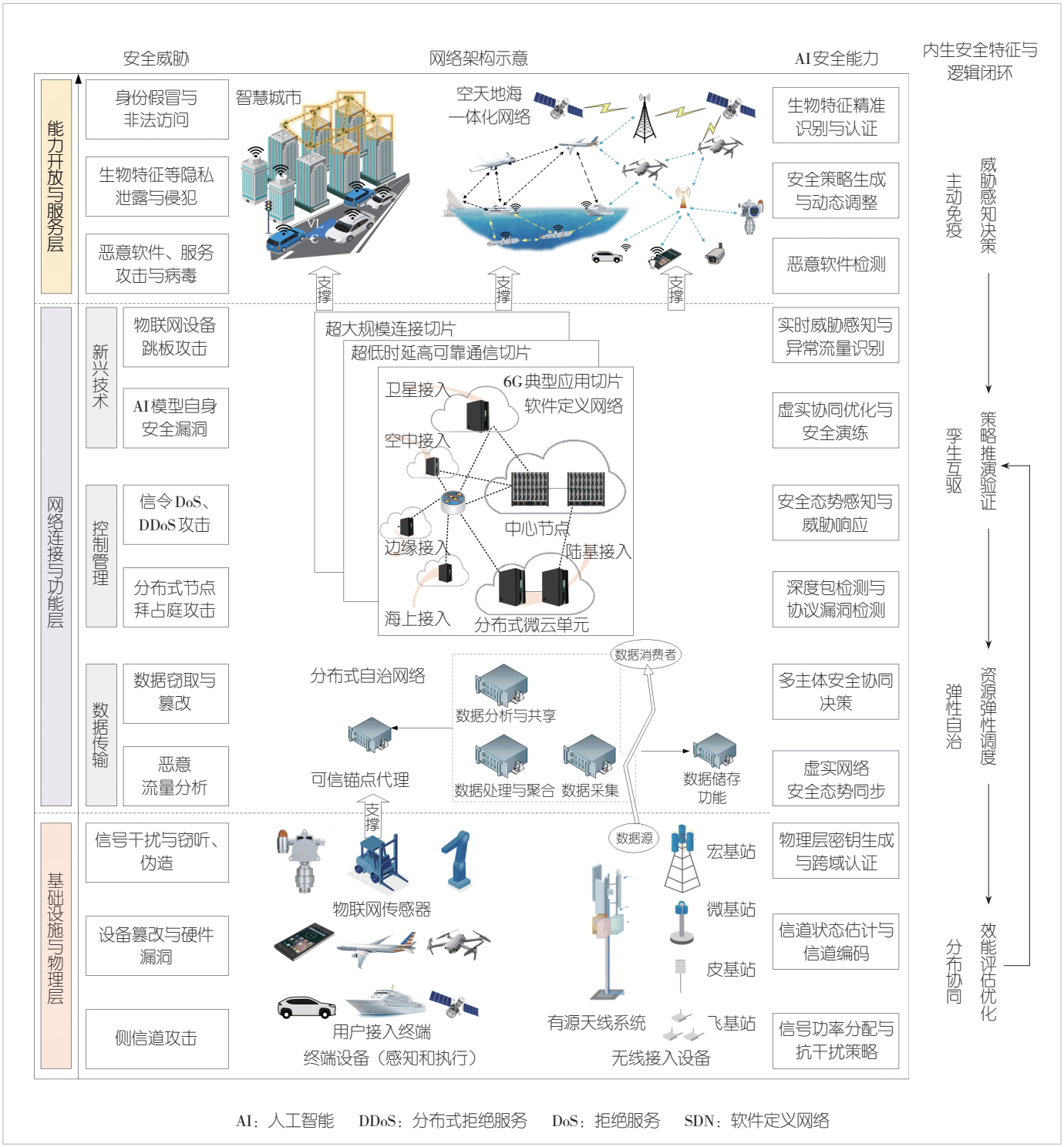
1）群体学习的横向协同防御机制

针对攻击面分散化特性，群体学习架构可构建完全去中心化的防御节点网络。基于点对点（P2P）协议搭建多跳通信链路，节点通过参数交互替代数据集中方式实现全局模型同步，在基站、终端及边缘节点间组建动态防御联盟。所采用的弹性共识机制赋予防御网络拜占庭容错能力，即便20%～30%的节点遭受APT攻击，仍可保障异常流量检测功能的持续运行。动态拓扑管理机制支持防御节点的灵活接入与退出，在基站切换、终端漫游等复杂场景下，持续推进入侵检测模型的迭代更新。

2）多智能体强化学习的纵向协同防御机制

针对跨域隐蔽攻击，多智能体强化学习架构可建立“感知–决策–执行”的纵向防御链条。物理层智能体实时监测射频指纹异常，网络层智能体解析流量时空特征，应用层智能体监测应用程序编程接口调用异常。基于Stackelberg博弈模型构建防御策略树，当检测到伪基站攻击时，物理层执行频谱迁移，网络层进行路由重配，应用层触发身份重认证。系统采用课程学习机制渐进增强防御力度，初期将误报率控制在5%以内以维持服务连续性，待攻击确认后全面启用防御策略。

3）联邦学习的隐私协同防御机制



AI：人工智能　DDoS：分布式拒绝服务　DoS：拒绝服务　SDN：软件定义网络

图1　AI赋能的6G网络内生安全架构

为应对跨域数据安全挑战，联邦学习框架可构建“数据不动模型动”的隐私保护范式。基于同态加密的梯度聚合框架支持多参与方（运营商、设备商、安全机构）协同训练0day攻击检测模型，同时严格保持各方漏洞数据库的物理隔离性。差分隐私技术的引入，可有效防止通过共享模型参数逆向推断特定用户通信行为特征。通过自适应加权联邦平均算法，协调异构防御节点的计算时延差异，在工业互联网场景中实现100 ms级的快速威胁响应。

表1 分布式机器学习算法范式

技术类型	基本特征	安全应用示例
群体学习	1）完全去中心化 2）弹性共识机制 3）动态拓扑管理	• 基于点对点流量特征训练全局异常检测模型，实现跨域分布式拒绝服务攻击检测 • 基于设备射频指纹识别与轻量级智能合约实现去中心化设备身份认证
多智能体强化学习	1）分布式决策 2）协同博弈优化 3）分层策略架构	• 各合法通信节点可协作选择通信频率，以抵抗具有频率感知能力的恶意设备攻击 • 在工业互联网中，可编程逻辑控制器捕获并交换攻击模式，实现安全态势感知、未知威胁防御与快速系统自愈
联邦学习	1）中心化协调 2）隐私增强 3）模型异构性支持	• 跨机构联合训练高级持续性威胁攻击检测模型，满足隐私合规要求 • 联合训练并优化太赫兹波束赋形参数，实现窄波束干扰智能识别与攻击 • 联合训练并优化太赫兹波束赋形参数，实现窄波束干扰智能识别与攻击抵抗

3.2 AI大模型

6G网络驱动万物智联向高阶形态演进的同时，也面临着跨模态深度伪造攻击、量子计算辅助破解及隐蔽性增强的APT攻击等新兴技术赋能的复合安全威胁。传统基于规则库或轻量级模型（如卷积神经网络、循环神经网络）的防御机制受限于静态知识边界与单模态感知能力，难以有效应对动态演化的复杂攻击。具备千亿级参数的AI大模型凭借其跨模态关联推理、小样本自主进化与生成式威胁模拟等核心能力，正逐步成为6G网络“智能内生安全”体系的关键技术支撑。在技术实现层面，安全大模型的构建通常基于通用基础模型进行安全领域适配：首先通过增量预训练方法将协议分析、物理层特征等跨域安全知识注入文本与多模态基座模型；其次结合提示工程技术与参数高效微调方法实现边缘计算场景的轻量化适配；最终通过通用能力与安全能力的双重评估体系进行优化，生成面向特定场景的定制化安全策略。图2展示了一种典型的安全大模型训练架构设计方案[9]。

该安全大模型构建了安全威胁表征空间，突破了传统特征工程对人工先验知识的依赖。典型应用包括：通过融合基站监控视频的光场特征与物理层信道状态信息，实现对AI生成深度伪造基站的精准检测；基于提示工程与强化学习的动态策略生成引擎，能将自然语言指令实时转化为防御动作，响应速度较规则引擎提升一个数量级[10]。相较于传统小模型，安全大模型的本质优势在于：

1）知识获取从“人工标注的单模态特征”转向“自监督的多模态关联”；

2）决策逻辑从“分类/检测原子任务”升级为“感知–推理–决策链”；

3）进化模式从“全量数据重训练”跃迁至“提示微调的分钟级适配”。

尽管面临算力消耗与实时性挑战，6G网络安全正朝着

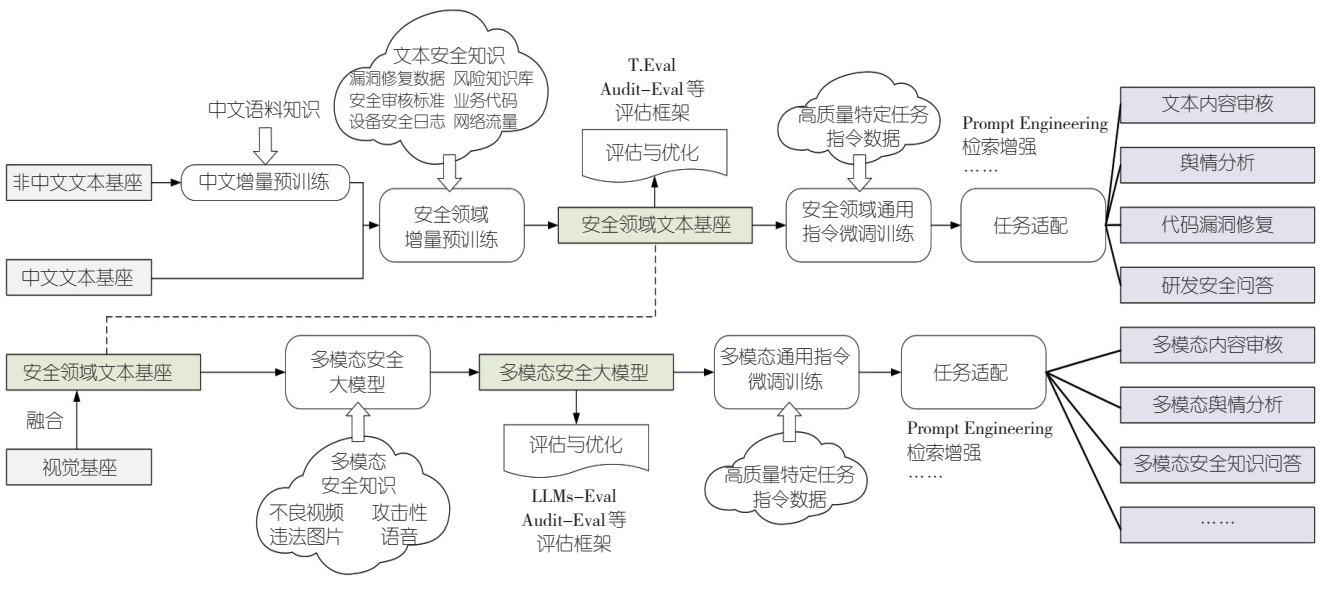


图2 安全大模型训练架构

基于轻量化边缘大模型（如混合专家系统架构）与多模态认知基座的技术路线演进，推动防御体系实现从“被动响应”到“威胁预判”的范式跃迁，最终达成深度防御、主动免疫与攻防自治的内生安全目标。

3.3 轻量级认证授权与访问控制技术

传统静态认证与基于网络边界的粗粒度访问控制在6G网络空天地海全域覆盖、超密集设备接入及高移动性场景下局限性日益凸显。新一代认证授权与访问控制技术以“持续验证、动态授权”的零信任等架构为支撑，基于密码技术革新实现抗量子与轻量化演进，并依托AI驱动的动态信任评估提升智能授权能力，主要体现在以下3个方面。

1） 认证机制从“凭证验证”向“上下文感知”演进

当前主流认证方案（如OAuth 2.0等）主要基于预置令牌或CA证书体系，存在量子计算破解与重放攻击隐患。6G网络通过融合设备硬件指纹、运行状态、用户行为模式及网络环境等多维上下文信息，结合抗量子轻量级密钥交换技术，实现资源受限终端的动态信任评估与安全认证[11-12]。典型方案包括基于格密码学的Crystals-Kyber协议，该方案在保持抗量子攻击能力的同时，其计算复杂度较公钥加密算法（RSA）降低一个数量级，可在边缘设备上完成毫秒级密钥协商，有效适配高移动性场景需求。

2） 访问控制从“边界授权”向“微隔离策略”演进

当前基于角色、属性、任务等的访问控制机制普遍存在颗粒度过粗的问题，而6G网络通过零信任架构能够实现动态化的最小权限访问控制：基于软件定义边界实现安全网关的隐形化，仅向已验证会话开放最小必要端口，并默认拒绝所有未显式允许的请求；同时利用图神经网络分析设备交互拓扑，识别异常连接模式，从而降低误报率。图3展示了一种6G场景下轻量级认证授权与零信任访问控制架构。

3） 架构从“中心化信任锚点”向“分布式认证网络”演进

现今常用的公钥基础设施（PKI）体系因中心化CA的单点故障与性能瓶颈，难以支撑数亿级设备并发认证。6G网络基于去中心化标识符，通过区块链与智能合约实现跨域设备身份自管理，可消除对中心化CA的依赖；基于门限签名技术，可将认证计算负载分散至边缘节点，实现亚毫秒级的边缘分布式认证。

上述技术演进主要致力于突破跨域信任传递与边缘算力约束的瓶颈，推动6G网络由“被动验证”向“无感认证”演进，最终实现“AI原生零信任”的安全架构。

3.4 数字孪生

传统安全机制采用单向的“检测-响应”模式（如防火墙规则更新、入侵检测告警等），本质上属于开环系统，缺乏对防御效果的持续验证与动态优化。而数字孪生技术将闭环控制理念深度整合至6G网络安全体系，通过“感知-决策-执行-验证”的实时反馈循环，实现了安全防御从开环到闭环的范式转变。网络安全数字孪生体系架构与双向映射逻辑如图4所示[13]。

在技术实现上，数字孪生通过实时同步物理层信号和协

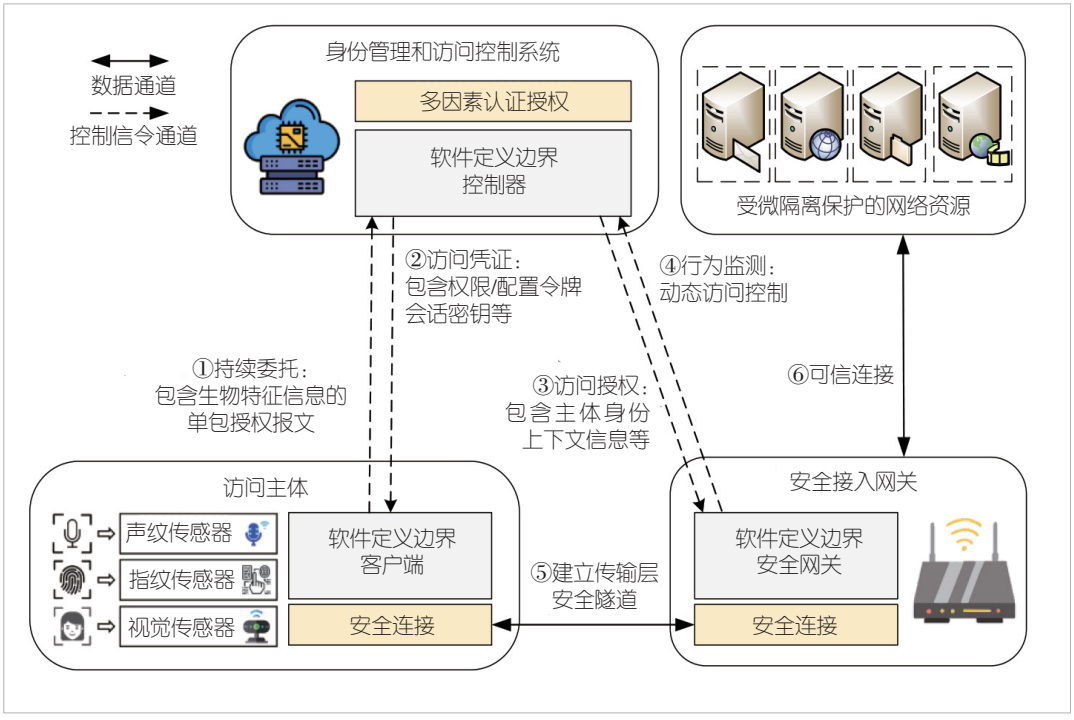


图3 轻量级认证授权与零信任访问控制架构

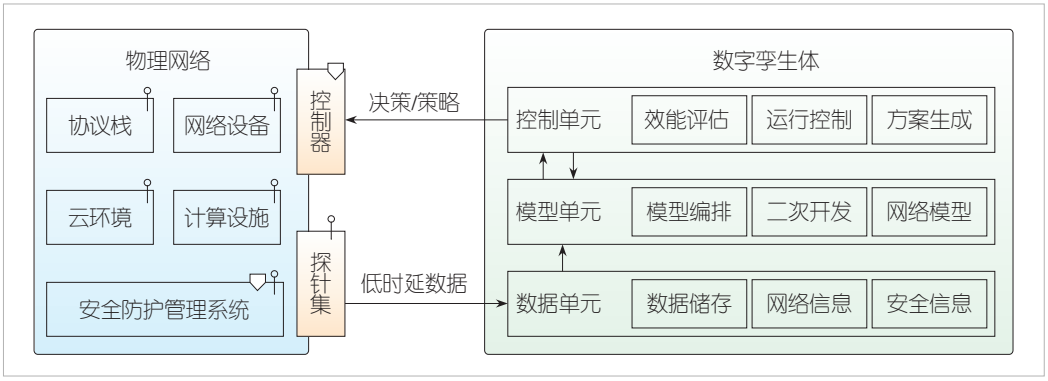


图4　网络安全数字孪生体系架构与双向映射逻辑

议流量等数据，在虚拟环境中模拟攻击传播路径并评估防御策略效果，通过A/B测试验证策略有效性后，再部署至物理网络，从而降低运维风险；同时，基于孪生反馈数据量化业务时延波动等防御副作用，有效提升了系统应对网络拓扑变化和攻击模式演进的适应能力。数字孪生的闭环安全技术链可描述如下：

1） 实时数据同步

利用网络遥测与时间敏感网络技术，实现物理网络与数字孪生体间的多维度状态同步，时延达到毫秒级，涵盖协议栈、设备状态及物理层信号等数据，为闭环控制提供低时延、高保真的数据支撑。

2） 虚拟推演与策略优化

采用离线–在线混合强化学习方法，在离线阶段通过历史数据预训练模型，在线阶段结合实时环境反馈，动态优化攻防博弈策略。

3） 闭环执行与验证

通过持续监测防御策略的执行效果及潜在副作用，基于贝叶斯网络构建因果推理模型，量化防御动作与网络状态变化的关联性，进而触发策略回滚或自适应更新。

数字孪生的闭环控制机制推动网络安全从“开环经验驱动”向“闭环系统科学”演进，其虚实协同的技术内涵显著超越传统仿真工具，成为6G实现内生安全的关键使能技术。

3.5 无线物理层安全技术

传统协议层安全机制依赖基于数学难题假设的加密算法，面临量子计算威胁且密钥管理复杂度随网络规模呈指数增长。相比之下，物理层安全直接利用无线信道的空间传输特性与硬件不可克隆性，实现无须预置密钥、低计算开销的空口安全防护。其核心创新在于将安全机制从协议层下沉至物理层，从基于数学难题的协议防护转向基于信道特征的智能防护，在降低算力与能耗的同时，构建“信号传输全链路免疫”的内生安全体系。在技术实现层面，无线物理层安全主要包含以下3项创新：

1） 基于信道特征的指纹动态密钥生成

基于深度学习实时提取信道状态信息的时空特征（包括多径时延分布、射频指纹及高速移动场景下的多普勒频移等），可生成实时更新的动态会话密钥，有效解决预置密钥的分发与管理难题，实现近似“一次一密”的安全传输[14]。该方案尤其适用于两类典型场景：（1）车联网、无人机群等高移动性场景，利用信道快速时变特性实现密钥动态生成，有效抵御窃听与重放攻击；（2）工业控制等敏感场景，通过一次一密机制保障关键指令传输安全，从根本上规避量子计算带来的长期密钥泄露风险。

2） 可编程智能反射面增强安全传输

通过编程调控超表面单元相位，RIS可实现三维波束精确赋形与窃听信道的主动干扰——合法用户接收主瓣增强信号，而窃听者则被约束在波束零陷或强噪声区域，通过物理层信噪比的差异化调控使截获信息无法有效解码[15]。

3） 新型通信介质实现原生性安全增强

太赫兹通信凭借其高方向性和低旁瓣特性，结合智能反射面技术，可抑制信号泄露并增强抗干扰性能[16]；可见光通信采用视距传输机制，其信号仅能在无障碍遮挡的直线路径上传播，从而降低非授权设备在传输过程中的截获概率[17]。

尽管在城市多径衰落和卫星轨道漂移等高动态环境下，信道特征的鲁棒性仍面临显著挑战，但无线物理层安全技术凭借其通信保密性和抗窃听优势，结合AI的智能处理能力，正推动6G网络安全从“信道加固”向“语义免疫”演进。

4 结束语

AI与6G网络的深度耦合正在重构网络安全的基础防护范式与技术体系。本文系统阐述了6G网络内生安全架构及其核心技术，基于分布式智能协同、动态信任评估和虚实闭环控制机制，成功应对6G异构环境下的新型安全威胁。然而，AI模型可解释性不足、算力实时性受限以及物理层安全鲁棒性欠缺等关键问题仍有待解决。未来研究应重点探索跨模态威胁建模、轻量化边缘智能部署及量子安全融合方向，推动6G网络安全实现从“被动防御”到“主动免疫”

的范式跃迁，为智能社会的数字化转型构建可靠的安全基座。

参考文献

[1] 张成磊, 付玉龙, 李晖, 等. 6G网络安全场景分析及安全模型研究 [J]. 网络与信息安全学报, 2021, 7(1): 28−45

[2] CAVIGLIONE L, GAGGERO M, LALANDE J F, et al. Seeing the unseen: revealing mobile malware hidden communications via energy consumption and artificial intelligence [J]. IEEE transactions on information forensics and security, 2016, 11(4): 799−810. DOI: 10.1109/TIFS.2015.2510825

[3] BOTHA M, SOLMS R, PERRY K, et al. The utilization of artificial intelligence in a hybrid intrusion detection system [EB/OL]. [2025−03−20]. https://dl.acm.org/doi/10.5555/581506.581527

[4] 蔡良伟, 程璐, 李军, 等. 基于遗传算法的正则表达式规则分组优化 [J]. 深圳大学学报理工版, 2015, 32(3): 281−289

[5] 粟栗, 庄小君, 杜海涛, 等. 6G网络内生安全架构研究 [EB/OL]. (2022−01−20) [2025−03−18]. http://scis. scichina. com/cn/2022/SSI−2021−0257.pdf

[6] 张秀贤, 朱晓荣. 6G网络中分布式AI模型协同技术综述 [J]. 移动通信, 2025, 49(1): 43−51

[7] 吴官翰, 贾维敏, 赵建伟, 等. 基于多智能体强化学习的混合博弈模式下多无人机辅助通信系统设计 [J]. 电子与信息学报, 2022, 44(3): 940−950. DOI: 10.11999/JEIT210662

[8] 王志勤, 江甲沫, 刘沛西, 等. 6G联邦边缘学习新范式: 基于任务导向的资源管理策略 [J]. 通信学报, 2022, 43(6): 16−27. DOI: 10.11959/j.issn.1000−436x.2022128

[9] 秦鹏达. 大模型让安全防护升级跃迁:如何让安全更加智能化 [EB/OL]. (2024−04−03) [2025−02−01]. https://mp. weixin. qq. com/s/GCijFpmdc0VbH−−R1tDsdA

[10] 田辉, 倪万里, 聂高峰, 等. 6G网络中面向AI大模型的联邦学习与协同部署技术综述 [J]. 移动通信, 2024, 48(8): 30−40

[11] CHAUDHRY S A, IRSHAD A, KHAN M A, et al. A lightweight authentication scheme for 6G−IoT enabled maritime transport system [J]. IEEE transactions on intelligent transportation systems, 2023, 24(2):2401−2410. DOI: 10.1109/tits.2021.3134643

[12] OMETOV A, BEZZATEEV S, MÄKITALO N, et al. Multi−factor authentication: a survey [J]. Cryptography, 2018, 2(1): 1. DOI: 10.3390/cryptography2010001

[13] 刘光毅, 邓娟, 郑青碧. 基于数字孪生网络的6G无线网络自治 [J]. 中兴通讯技术, 2023, 29(3): 2−7

[14] 戴峤, 宋华伟, 金梁, 等. 基于等效信道的物理层认证和密钥分发机制 [J]. 中国科学: 信息科学, 2014, 44(12): 1580−1592. DOI: 10.1360/N112013−00041

[15] 朱政宇, 王梓晅, 徐金雷, 等. 智能反射面辅助的未来无线通信: 现状与展望 [J]. 航空学报, 2022, 43(2): 203−217. DOI: 10.7527/S1000−6893.2021.25014

[16] 陈智, 刘轲, 李玲香, 等. 太赫兹通信感知一体化技术综述 [J]. 中国科学: 信息科学, 2024, 54(5): 1215−1235. DOI: 10.1360/SSI−2023−0354

[17] 施剑阳, 牛文清, 徐增熠, 等. 面向6G的可见光通信关键技术 [J]. 无线电通信技术, 2021, 47(6): 692−697. DOI: 10.3969/j.issn.1003−3114.2021.06.003

作 者 简 介

王瀚洲，北京航空航天大学在读博士研究生；主要研究领域为信息网络安全、网络化系统安全与隐私保护。

金子安，北京航空航天大学在读博士研究生；主要研究领域为6G内生安全、人工智能安全。

王瑞，北京航空航天大学在读博士研究生；主要研究领域为6G内生安全、空天地一体化网络安全等。

刘建伟，北京航空航天大学网络空间安全学院创院院长、教授、博士生导师，国家级教学名师，享受国务院政府特殊津贴专家，现任国务院学位委员会学科评议组成员、教育部网络空间安全专业教学指导委员会委员、中国密码专业学位研究生教学指导委员会委员、中国密码学会常务理事、中国指挥与控制学会常务理事、中国电子学会网络空间安全专委会副主任委员、中国指挥与控制学会网络空间安全专委会副主任委员等；主要从事网络空间安全领域的科研和教学工作；曾获国家技术发明奖一等奖、国防技术发明奖一等奖、中国指挥与控制学会科技进步奖一等奖等，所编著的教材获评全国普通高校优秀教材一等奖、国家网络安全优秀教材奖、普通高等教育国家级规划教材、普通高等教育精品教材、全国优秀科普作品奖、第四届中国科普作家协会优秀科普作品金奖等；发表论文200余篇，获授权技术发明专利120余项，主编教材16部、专著7部、译著1部。