中国科学 : 信息科学 2025 年 第 55 卷 第 8 期: 1801–1821
SCIENTIA SINICA Informationis
网络韧性理论与技术专题 · 论文

6G 核心网韧性体系: 愿景、架构与关键技术

季新生[1,2], 廖星星[2*], 杨杰[1], 游伟[1], 王子龙[3], 李聪[3], 邱航[1], 冯润涵[2]

1. 国家数字交换系统工程技术研究中心, 郑州 450002
2. 紫金山实验室, 南京 211111
3. 西安电子科技大学网络与信息安全学院, 西安 710071
* 通信作者. E-mail: liaoxingxing@pmlabs.com.cn

收稿日期: 2025–02–10; 修回日期: 2025–05–26; 接受日期: 2025–07–01; 网络出版日期: 2025–08–08

国家重点研发计划 (批准号: 2022YFB2902204)、河南省顶尖人才培养计划 (批准号: 244500510012)、河南省重点研发专项 (批准号: 231111211000) 资助项目

摘要 作为支撑人机物三元融合社会的数字基础设施, 第六代移动通信系统 (6G) 呈现出开放异构、云网融合、智慧内生等复杂特性. 网络韧性作为 6G 系统的一项关键内在质量属性, 对于确保其在复杂环境下的持续可靠运行至关重要. 本研究通过系统分析 6G 网络韧性研究动态与技术演进趋势, 在内生安全理念指导下提出了一种 “3-3-4-4-2” 框架下的核心网韧性体系构想. 该构想旨在应对开放环境高级持续威胁、云化网络功能失效风险和多域流转隐私数据泄露三大核心挑战, 通过构建 “点 – 线 – 面” 三维韧性增强机制, 系统集成多维感知、动态修复、迭代更新和灵活包容四项核心能力, 从而达成预测与智能优化、抵抗与故障容错、快速响应与恢复及自适应自演化四项韧性目标, 并形成具备可测试、可验证特征的韧性评估体系. 基于该构想, 本文进一步提出了具有工程可行性的 6G 核心网韧性参考架构, 深入阐释其协同工作机制与动态演化原理, 并识别了多项候选关键技术, 为构建具有内生韧性的 6G 网络提供理论支撑与技术实现路径.

关键词 6G, 核心网, 网络韧性, 协同安全, 评估体系

1 引言

人们普遍认为, 作为下一代支撑人类社会的关键信息基础设施, 6G 网络将融合人、机、物三元世界 [1], 并催生出具有复杂系统特征的数字生态系统. 这种深度互联的特性不仅带来风险的多维度叠加, 更可能引发跨域风险的级联放大效应. 鉴于其地位的特殊性, 国际标准组织与头部科技企业在 6G 架构设计之初即高度重视安全体系构建. 美国 6G 研究组织 NGA (Next G Alliance) 在其 6G 路线图 “Roadmap to 6G” 报告中, 把可信、安全和韧性 (trust, security, and resilience) 列为其 6G 六大目标之首 [2]. 欧盟智能网络和服务联合体资助了一系列 6G 项目, 其中与可靠服务和智能安全相关的项目有 iTrust6G, NATWORK, ROBUST-6G, SAFE-6G 等, 这些项目优先考虑用户数据保护和隐私、可靠

引用格式: 季新生, 廖星星, 杨杰, 等. 6G 核心网韧性体系: 愿景、架构与关键技术. 中国科学: 信息科学, 2025, 55: 1801–1821, doi: 10.1360/SSI-2025-0059
Ji X S, Liao X X, Yang J, et al. 6GC cyber resilience: vision, architecture, and key technologies. Sci Sin Inform, 2025, 55: 1801–1821, doi: 10.1360/SSI-2025-0059

性、信任和弹性, 目的是确保安全过渡到 6G [3]. 下一代移动网络联盟 NGMN 于 2023 年 10 月发布 6G 安全愿景白皮书 *6G Trustworthiness Considerations*, 聚焦 6G 的安全可信赖性. 白皮书首先分析了 6G 安全可信赖性的 4 个驱动力 —— 社会需求、网络演进需求、业务驱动需求, 以及安全技术驱动需求 [4]. 诺基亚贝尔实验室在 *Security and Trust in the 6G Era* 白皮书中将安全、隐私和信任提升为 6G 研究的首要领域 [5]. 需要指出的是, 在探讨 6G 的安全特性时, 除了传统的通信安全和隐私保护外, 更加强调确保服务连续性的 "使命保障" 能力, 即 "韧性". 这意味着系统必须能够在遭受网络攻击或其他挑战时, 依然保持关键业务的稳定性和可靠性, 确保不间断的高质量服务.

韧性原本是物理学概念, 指事物受干扰后保持最低限度能力并恢复或弹回到原来状态的能力, 还可以理解为应变体在由压缩应力引起形变之后保持最差机能并恢复其大小和形状的能力. 随着网络安全威胁愈演愈烈, 欧美在系统工程、信息技术和计算机网络领域也逐渐引入了 Resilience 概念. 国内学者将 Resilience 翻译成韧性或弹性, 表达的意思既包含准备好应对并适应变化条件, 也包括经受故意攻击、意外事件或自然灾害的破坏后, 从中迅速恢复的能力. 近年来, 随着对这些能力需求的增长, 韧性研究已成为业界关注的一个热点领域. 2021 年 12 月, 美国国家标准与技术研究院 (NIST) 发布了 "Developing cyber-resilient systems: a systems security engineering approach", 将网络弹性定义为包含网络资源的实体所具备的对各种不利条件、压力、攻击或损害的预防、抵御、恢复和适应能力 [6]. Akinsanya 等 [7] 在 2024 年系统回顾了网络弹性概念的演变, 通过深入探讨风险评估、威胁情报、事件响应和恢复计划等关键组成部分, 揭示了这些要素如何协同工作以提高组织防御和恢复能力. Zhu 等 [8] 探讨了融合控制理论、博弈论和机器学习 3 种理论用于设计网络弹性机制, 以实现对威胁的自主和自适应响应. Li 等 [9] 基于分层 Petri 网对 5G 用户面进行建模, 并度量评估了应对网络异常流量下不同扩缩容以及网络隔离等资源调度策略下的网络韧性. 面向 6G 领域, 欧美等在规划安全愿景时, 普遍将韧性作为重要考量, 期望 6G 在自然灾害、故障或网络攻击下维持稳定服务, 即使无法避免服务受损, 也能够有序降级并迅速恢复. 在此背景下, 美国自然基金委 [10] 启动的韧性智能的下一代网络项目 RINGS, 强调要在下一代网络的各项赋能技术中均需考虑设计安全、自主恢复和高度灵活适应性. 德国 Open6GHub 项目 [11] 强调要在 6G 的无线、边缘、核心网和云设施等所有层面都加强 "自我意识"、自我重配置和自我保护等网络韧性设计. NGA [12] 提出了可信网络的生命周期全景图, 利用包括人工智能在内的先进技术, 在网络的开发、部署、(重) 配置以及运维等环节中实施相应的措施来增强网络的韧性.

然而, 值得注意的是, 现有韧性研究以强恢复视角为主, 强调采用事先多做预防、事后尽快弥补恢复的策略. 这类方法本质上依赖对已知威胁的认知, 在面对未知攻击 (尤其是具备隐蔽性的高级持续性威胁 (advanced persistent threat, APT)) 时, 难以在网络遭受首次冲击期间维持关键业务连续性. 这一局限性在 6G 人机物融合场景中尤为突出, 即使网络能在事后快速恢复, 单次短时中断造成的损失亦不可逆. 为解决传统韧性研究对未知攻击的防御局限, 邬江兴院士及其团队 [13] 提出了具有 "结构决定安全" 属性的内生安全构造, 即动态异构冗余架构 (dynamic heterogeneous redundancy, DHR), 能够在不依赖先验知识前提下有效抑制系统内存在的 "已知的未知""未知的未知" 异常扰动导致的不利影响, 进而赋能网络系统具备网络韧性. 文献 [14] 则进一步阐述了内生安全构造在网络韧性整个生命周期的赋能方法.

基于上述分析, 6G 网络韧性设计需突破传统 "事后恢复" 的被动模式, 转而构建首次攻击免疫能力, 即在遭遇 "未知的未知" 攻击时, 仍能通过内生安全机制保障核心功能的持续运行. 这一目标的实现需与 6G 架构演进路径深度耦合. 当前, 尽管 6G 网络架构尚未形成统一标准, 但在工业互联网、沉浸式 XR 等多样化场景驱动下, 全服务化架构与 "云 – 边 – 端 – 网" 协同的分布式自治架构已被普遍视为核心演进方向 [15~17]. 上述架构在带来服务能力提升的同时也为韧性网络构建带来了挑战. 值得注意的是, 现有研究虽围绕 6G 安全愿景 [4]、可信接入 [18]、隐私增强 [19] 等方向取得一些成果, 但总体上多聚焦于传统安全范畴, 在如何实现 "攻而难倒" 的网络韧性目标、如何与 6G 核心网架构协同

设计方面尚缺乏足够关注. 针对上述问题, 本文深入探讨了韧性视角下 6G 核心网需应对的挑战, 进而在内生安全理念指导下提出 6G 韧性体系构想, 涵盖防御维度、关键能力、核心目标、度量验证等方面. 进一步, 基于该构想, 提出了一种韧性参考架构, 并阐述了其工作机制. 同时, 识别并分析了潜在韧性赋能技术, 以期为达成上述目标提供理论支撑.

2　韧性体系构想

ITU-R 已明确 6G 六大典型场景, 包括沉浸式通信、超大规模连接、极高可靠低时延通信、AI 与通信融合、通感一体和泛在连接 [20]. 多场景、多网络、多技术之间的融合, 使得 6G 网络系统构成了一个复杂巨系统. 该系统涉及人与人、人与物、物与物之间的感知、计算、通信及控制过程. 系统网络安全风险也面临着多样性、复杂性和不可预见性. 作为移动网络的大脑, 核心网长期以来面临着高稳、高效和业务创新使能等挑战. 在 6G 核心网架构演进中, 网络韧性作为内生的质量属性, 其构建需要系统性应对新型技术引入和网络部署模式变革 (如分布式架构、云边端深度协同) 带来的双重安全挑战. 文献 [21] 从复杂系统理论角度出发, 强调网络安全韧性是系统各组件相互作用产生的涌现行为, 突破了传统仅关注单独组件的网络安全实践和成熟度模型的局限, 为 6G 核心网韧性体系提供了从行业层面、系统整体相互依赖性角度构建理论架构的新思路, 启发我们在 6G 核心网韧性研究中, 不应孤立看待各网络环节, 而要考虑其复杂关联性. 本节从韧性视角出发, 首先识别核心网面临的三大典型安全威胁, 进而提出核心网韧性体系构想, 并深入剖析该体系所具备的关键能力、核心目标, 以及相应的测试与评估方法.

2.1　核心网韧性视角下安全威胁

文献 [22] 给出的混合威胁模型和分析方法, 以及开发的自动化工具 TAMELESS, 拓宽了对威胁的认知视角. 在 6G 核心网韧性体系研究中, 应借鉴这种多维度考虑威胁因素的方式, 综合分析网络层面、物理基础设施层面以及人为因素等方面可能存在的安全隐患, 构建更全面的威胁模型, 使 6G 核心网能够更有效应对复杂多变的威胁环境.

为适应未来多样化场景需求, 6G 核心网架构演进呈现两大特征: (1) 通过全服务化架构实现网络功能的深度解耦; (2) 采用分布式自治组网模式推动网络能力下沉. 这种架构演进在提升服务灵活性的同时, 也带来三方面安全挑战: 首先, 云化/开源组件的不可信多源供应链导致软硬件漏洞风险加剧; 其次, 核心网切片的开放服务化接口显著扩大攻击面; 最后, 在网络产品设计过程中, 设计者不严格遵守安全设计原则或未充分考虑安全性, 可能引入未知的漏洞. 因此, 6G 核心网韧性的设计必须从根本上解决这一问题, 致力于在即使遭遇 “未知的未知” 等网络攻击时仍能有效避免损失, 维持核心功能提供有效服务. 具体而言, 如图 1 所示, 6G 核心网需应对以下三类威胁.

开放环境高级持续威胁. 指由于核心网软件 IT 化后与多样化供应链交织, 攻击者利用网络基础设施的隐蔽后门或零日漏洞, 实施多阶段 APT 攻击, 导致 6G 网络服务中断或性能下降的威胁. 可能性包括网络边界中的接入点、远程访问技术的使用, 进入组织网络基础设施的受感染文件. 如攻击者可利用第三方虚拟网络功能 (virtual network function, VNF) 组件存在的未授权访问漏洞, 导致恶意流量穿透网络隔离策略, 造成严重网络事故.

云化网络功能失效风险威胁. 6G 核心网采用云原生架构后, 各层级组件因设计缺陷或运维失当引发的系统性服务风险. 例如, 基础设施层虚拟化资源调度异常导致网络功能虚拟化 (network functions virtualization, NFV) 实例资源争用 (如节点亲和性配置错误引发的 vCPU 超分配), 编排层服务网格流量策略冲突造成网络功能链断裂 (如虚拟服务路由规则矛盾导致的用户面数据丢包), 以及服务层微服务依赖关系失衡引发的级联故障 (如服务化架构中网络存储功能异常引发的全网服务注册失效).

多域流转隐私泄露威胁. 指在 6G 分布式网络架构下, 通感数据、用户签约信息等敏感数据在跨

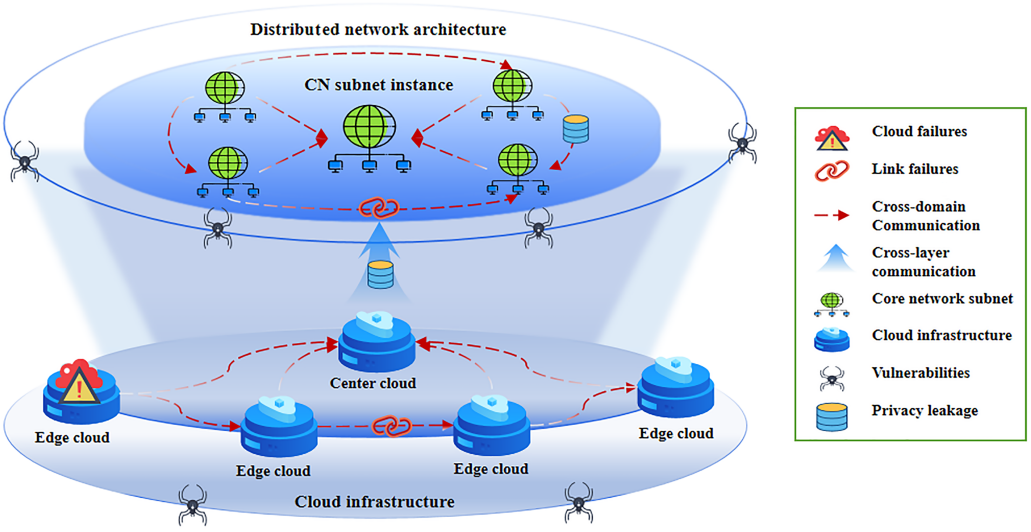

图 1　(网络版彩图) 6G 分布式网络面临的安全威胁示意图.

Figure 1　(Color online) Schematic illustration of security threats in 6G distributed network architecture.

自治域传输过程中, 隐私信息遭受中间人攻击或数据篡改, 进而引发网络服务功能异常或服务质量劣化的安全风险. 以混合组网场景为例, 攻击者通过控制边缘子网节点, 可实施两类破坏行为: (1) 篡改用户身份标识及位置信息, 致使合法用户被网络拒绝接入; (2) 伪造网络服务选择策略, 非法提升用户权限等级, 获取本应受限的高价值服务访问权.

2.2　韧性体系构想设计

针对上述三类威胁, 如图 2 所示, 给出了 6G 核心网韧性体系. 该体系综合考虑了 6G 网络的各个关键要素, 包括物理基础设施、虚拟化网络资源、网络服务编排与管理, 确保从单一网络功能到整个网络系统的全面韧性. 同时从 3 个维度进行综合防护: 网络功能、网络流程和链路, 以及网络架构, 也即点、线、面.

点: 指增强 6G 网络功能的韧性能力. 依据动态异构冗余架构设计 6G 网元 (虚拟化或实体), 当系统发生故障时, 冗余配置的部件可作为备份, 及时介入并承担故障部件的服务, 避免因单点故障而造成业务中断的情况. 当设备受到攻击后无法保持正常工作状态时, 可切换到最低业务系统能力保障核心业务的连续性. 当网络面临突发流量时能够自动伸缩以保障业务的服务质量.

线: 指在网络链路和流程上保证 6G 网络韧性. 通过链路冗余、逃生路径、韧性选路等方式, 当网元受到非法攻击时, 网络可以主动将其旁路或进行业务迁移或切换, 确保网络服务的可用性. 通过不同类型的网络备份, 当受到攻击或自然灾害时, 可继续保障业务的稳定运行.

面: 指在架构上保证 6G 网络韧性. 借鉴动态异构冗余的构造思想, 使用多设备、多系统、多网络改变现有业务系统组成的相似性、单一性, 在业务系统受到攻击或故障时能灵活改变业务的承载设备、系统类型和网络路径, 保持业务稳定运行, 提供可靠的服务. 同时, 通过部署具备自包含特性和智能决策能力的网络功能单元, 形成分布式自治拓扑结构, 在局部节点受损时, 相邻单元可快速重构服务链路, 有效保障全域服务的持续可靠运行.

在此基础上, 通过实施负载均衡、冗余设计、动态切换、意图识别和智能协同等措施, 构建一个冗余、异构、自监督、自适应和自生成的 6G 核心网韧性体系, 并促进形成一个具备多维感知、灵活包容、动态修复和迭代更新能力的网络系统. 系统横向层面能够与其他安全防护技术或体系融合, 形成协同防御机制. 纵向层面能够与智能网联基础平台之上的其他技术体系融合, 形成韧性自治的能力.

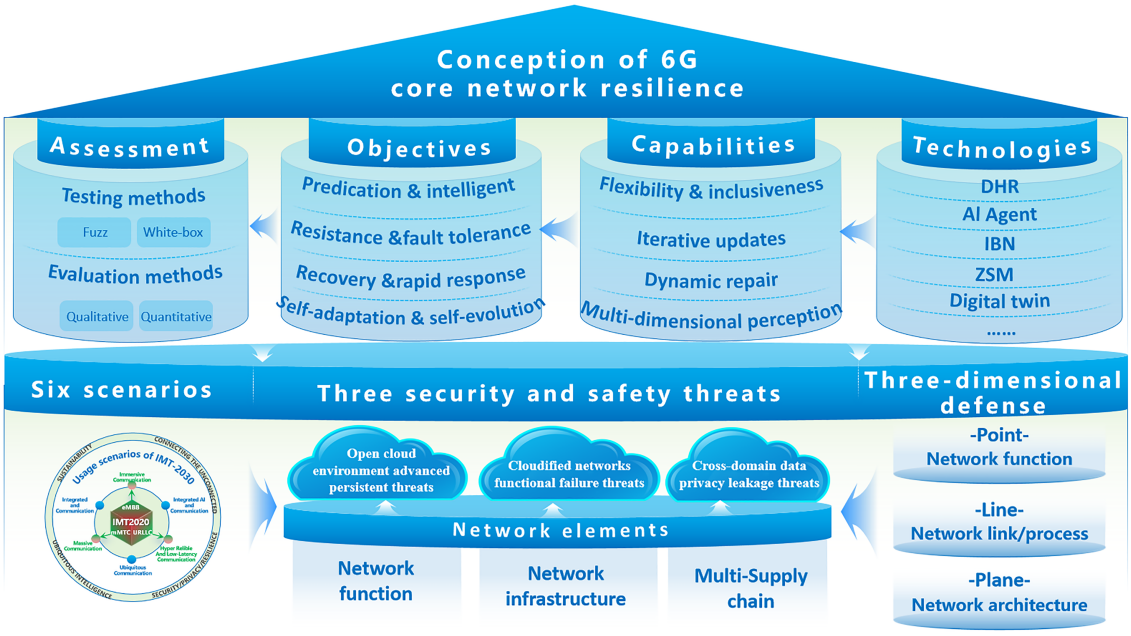

图 2　(网络版彩图) 6G 核心网韧性体系构想.

Figure 2　(Color online) Resilience framework conception in 6G core networks.

通过这种方法, 形成覆盖 “风险预测与智能优化 → 攻击抵抗与故障容错 → 服务恢复与快速响应 → 系统自适应与架构自演化” 全生命周期, 并具备可测试、可评估的智能韧性体系.

2.3　韧性关键能力分析

关键能力 1: 多维感知 (multi-dimensional perception, MP). 在 6G 网络中, 系统运行和业务处理伴随着海量数据的生成, 构建网络韧性能力的关键在于对这些数据进行多维度感知. 多维感知涵盖横向感知、纵向感知和时空感知 3 个层面. 横向感知聚焦业务全生命周期管理, 通过终端设备、边缘节点、核心网元的全链路数据采集, 建立从用户需求感知到服务交付验证的闭环监测机制, 有效支撑业务质量溯源和异常行为检测. 纵向感知贯穿云 – 边 – 端协同架构, 基于虚拟化平台运行状态、容器编排日志及开源组件安全信息的深度整合, 形成覆盖基础设施层、平台层、应用层的立体化监控体系, 重点应对多供应商环境下的供应链安全风险. 网络威胁情报收集、分析与利用十分重要, 及时掌握潜在威胁信息, 有利于提前做好防御策略规划, 提升网络的主动防御能力和韧性 [23]. 时空感知通过融合环境传感器网络与数字孪生建模技术, 结合气象演变、地理特征与网络拓扑的动态关联分析, 构建具备趋势预测能力的智能模型, 可对自然灾害、社会事件等复杂场景进行空间推演和影响评估.

关键能力 2: 动态修复 (dynamic remediation, DR). 动态修复是提升 6G 核心网韧性的核心技术之一, 它融合了分布式自治、跨域协同及人工智能等多种先进技术, 实现了网络资源的高效利用、自动化的资源分配与优化, 从而增强了网络应对流量高峰、网络攻击或自然灾害等挑战时的适应性和恢复力. 例如, 6G 网络可以自动检测并定位故障服务节点, 迅速识别并防御网络攻击, 以及在基础设施受损时快速部署新的网元或进行跨云协作, 确保高级别通信服务的连续性. 这种特性促使 6G 核心网的韧性从被动、间歇性向主动、持续性转变, 赋予网络先天的防御能力和后天学习得来的经验式修复能力, 以提升复杂场景下的服务连续性保障水平.

关键能力 3: 迭代更新 (progressive updates, PU). 迭代更新是指 6G 核心网网络能够不断学习系统运行知识, 优化自身功能结构, 进而适应新的威胁与挑战. 迭代更新体现在两个方面: 一是优化业务服务质量, 二是调整网络状态或集成新技术, 以适应外部环境变化或抵御新出现的漏洞威胁. 迭

代更新可通过在数字世界中对物理实体或过程进行模拟、验证、预测和控制, 获得物理世界的最优状态, 实现从 “恢复” 到 “免疫” 的跃迁.

关键能力 4: 灵活包容 (flexible integration, FI). 作为复杂的巨型系统, 6G 网络在架构层面上需要兼容不同的技术, 在业务层面上需满足差异化的韧性需求. 这要求 6G 网络是一个高度可扩展、可编程且模块化的系统, 支持新兴技术和服务的快速部署和演进, 从而实现按需定制、动态部署和弹性伸缩的网络韧性能力. 一方面, 通过网络功能 API 和标准化接口, 第三方开发者可以以创新的方式与网络互动; 另一方面, 可编程能力应超越数据平面, 延伸至控制平面. 开放程度取决于是否能有效利用 3GPP CAPIF (common API framework, 通用 API 框架)、ETSI SDN (软件定义网络) 控制器等框架来为网络部署和连接、资源编排管理、服务和应用提供支持.

2.4　韧性核心目标解析

核心目标 1: 预测与智能优化 (prediction and intelligent optimization, PIO). 预测是网络韧性的第一道防线, 它基于多维感知能力实现对潜在威胁的前瞻性认知和评估, 并对威胁可能发生的时间、地点和方式进行预测. 在 6G 核心网智能韧性体系内, 预测能力至关重要. 它基于对历史安全事件的深入分析、用户行为的分析、系统漏洞的评估、网络状态趋势的监测以及异常流量模式识别, 确定网络哪个环节最有可能成为攻击的目标, 并确保这些节点得到适当的保护. 通过在数字世界中对攻击过程进行模拟、验证, 网络可以不断优化其预测能力, 确保能够及时发现新的威胁并响应.

核心目标 2: 抵抗与故障容错 (prevent and fault tolerance, PFT). 抵抗与故障容错是网络韧性的第二道防线, 它通过对攻击影响的控制和限制或对攻击者行动的遏制, 能够在一定程度上保持关键服务的质量和性能. 这涉及对硬件故障、软件错误、网络问题等各种异常情况的处理. 常见的容错机制包括冗余备份、数据镜像、错误检测与纠正等. 同时, 借助内置的冗余机制和自愈能力, 6G 网络能够自动检测和响应故障, 快速重新配置资源, 修复受损服务, 确保用户体验的无缝性和业务运营的持续性. 6G 网络通过有效的防御体系和冗余机制, 可以提高自身的鲁棒性, 实现对威胁承受和容错能力.

核心目标 3: 快速响应与恢复 (rapid response and recovery, RRR). 快速响应与恢复是 6G 核心网韧性的核心要求, 强调在网络遭受攻击后迅速恢复正常运作. 为了实现这一目标, 需要制定详尽的灾难恢复计划和业务连续性计划, 包括数据备份策略、系统恢复点创建、关键业务功能优先级排序以及设定恢复时间目标和数据恢复点目标. 6G 网络韧性涵盖多个相互交织的实现策略, 这些策略共同构成面临不断变化的网络威胁和挑战时能够自我监督、自我保护、自动适应并迅速恢复的全方位防御体系.

核心目标 4: 自适应与自演化 (self-adaptive and self-evolving, SASE). 自适应与自演化是网络韧性的最终目标. 6G 核心网应被视为一个动态进化的过程, 它模仿生物进化的原理, 使各组件能够自我学习和进化, 以适应外部环境的变化, 并应对不断演变的安全威胁. 这不仅要求网络根据历史数据和实时威胁情报自动调整安全设置和策略, 还需具备识别新威胁模式和自动更新防御措施的能力. 此外, 自适应能力还要求网络能够快速响应新的用户需求. 这可能涉及软件更新的自动化部署, 以及对网络设备的自动配置. 通过这种方式, 网络不需要手动干预, 实现零接触网络目标.

2.5　韧性测试评估属性解构

6G 核心网韧性需满足可测试性与可评估性两大核心属性, 并需从两个维度切入: (1) 针对不同威胁类型设计动态适配的测试方法, (2) 结合 6G 业务场景需求扩充评估标准, 确保韧性能力既能应对已知风险, 也能适应未知挑战.

2.5.1　可测试属性

在网络韧性测试方法方面, 根据威胁的认知程度, 可采用不同的测试方法.

针对 “已知的已知” 威胁, 即对于可以提前预想到的网络系统故障, 可以采用混沌测试这一测试方法. 混沌测试通过主动向系统注入预设故障 (如随机关闭网元、模拟流量过载), 观察系统在异常状态下的行为表现. 其目的是验证系统架构的容错性, 验证系统在压力测试下的韧性, 并通过优化架构和资源调度策略提升故障免疫力. 例如, 在 6G 核心网中, 可随机触发部分网元失效, 检测业务恢复时间和数据一致性是否达标.

针对 “已知的未知” 威胁, 典型的是在网络安全场景下, 当系统中存在未知漏洞且可能被攻击者利用时, 模糊测试是一种有效的检测手段. 模糊测试通过向系统输入异常数据 (如畸形协议包、非标接口请求等) 来模拟攻击者可能使用的技巧, 目的是发现潜在的安全漏洞和错误. 该方法不仅能揭示系统中的潜在安全漏洞, 还能间接评估系统在面对异常流量时的稳定性和可靠性. 例如, 通过对 6G 通感接口构造某些异常输入可能导致关键服务降级策略被触发, 进而影响服务质量.

针对 “未知的未知” 威胁, 即面对那些尚未预见的新型威胁, 可以采用白盒测试方法. 该方法通过开放部分可重构执行环境, 允许攻击者在可控范围内尝试突破系统防御, 从而验证系统架构对未知攻击的主动防御能力. 例如, 在 6G 网络切片场景中, 测试攻击者能否通过局部漏洞劫持全局资源.

2.5.2　可评估属性

6G 核心网韧性评估度量需面向 6G 潜在愿景在现有国标《信息安全技术网络弹性评价准则》[24] 定义的韧性指标基础上进一步扩展, 形成多维度动态评价体系. 一方面, 继承传统故障恢复时间、业务降级平滑度等指标, 同时新增 6G 特性指标, 包括空天地多接入协同效率、AI 自治决策可靠性、通感融合服务一致性等. 另一方面, 根据业务重要性 (如应急通信、工业控制) 设定差异化韧性阈值; 针对复杂场景 (如算力网络、语义通信) 引入动态权重, 确保评估结果与业务实际需求匹配.

在评估方法上, 主要采用基于系统架构的网络韧性评估框架 [25], 通过定义网络韧性系统架构关键性质、核心能力和主要指标, 对系统架构的网络韧性能力进行评估. 具体实施包含三阶段方法: 高层次定性评估侧重识别架构级缺陷; 定性 – 半定量覆盖式评估通过攻击树模型量化威胁路径阻断率; 详细定量评分评估则对设计的韧性指标进行加权计算. 验证阶段需融合混沌测试、模糊测试及白盒测试, 形成韧性能力闭环验证. 需强调的是, 系统架构的韧性基座能力决定整体上限 —— 若系统架构的某一评价要点得分过低, 如信令平面隔离度, 即便叠加冗余技术也难以保障核心业务韧性.

3　韧性参考架构

基于上述构想, 以及构造决定安全的理念, 我们致力于探索 6G 云网融合场景下的网络韧性增强机制, 并通过空间、技术和供应链层面实现多样性, 达成韧性架构的设计.

3.1　韧性架构设计框架

如图 3 所示, 6G 核心网韧性参考架构将动态性、异构性和冗余性作为其设计的核心, 同时整合了包括安全检测、威胁感知、意图识别、信任评估在内的多种先进安全技术. 通过运用多设备、多系统和多网络的协同效应, 使得网络在遭受攻击或出现故障时, 能够灵活地调整承载设备、网络路径和系统结构, 从而提供韧性服务. 参考架构包含 3 个层次: 异构云基础设施层、网络韧性使能层、韧性网络功能层.

异构基础设施层: 作为物理底座支撑层, 提供多维资源融合供给能力. 该层通过整合不同厂商的硬件和软件资源, 构建了一个高度容错和分布式的云环境. 高度容错设计使其能够容忍组件失效而保护 6G 网络免受单点故障的影响; 分布式架构设计使得计算任务和数据存储可以在多个地理位置的云

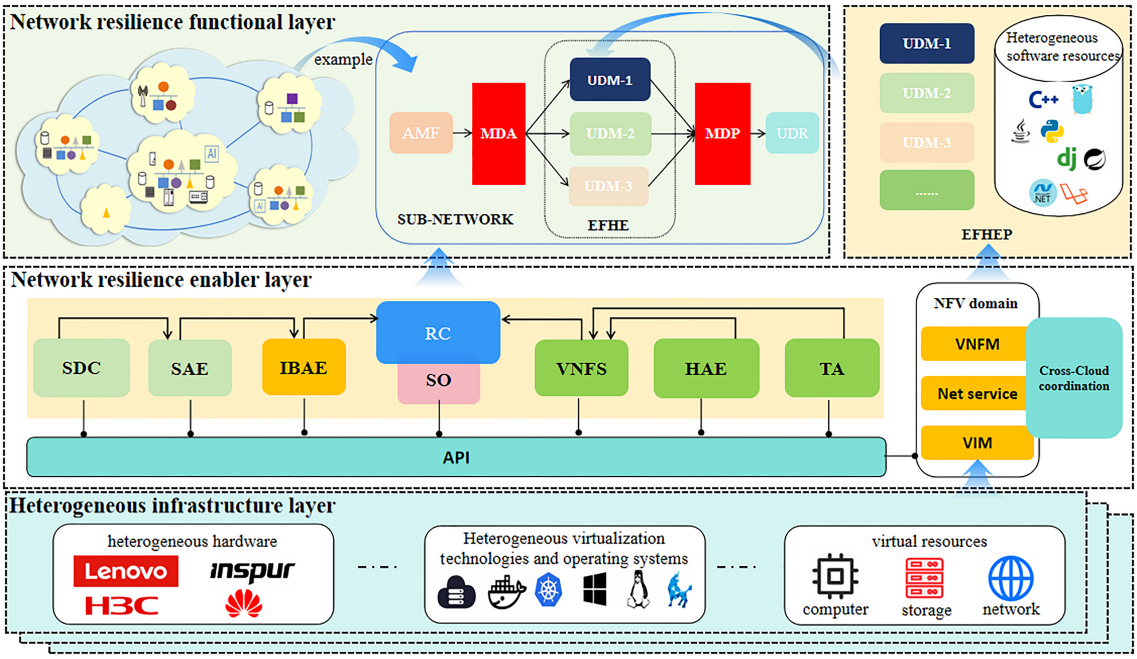

图 3　6G 核心网韧性参考架构.

Figure 3　(Color online) Resilience reference architecture for 6G core networks.

节点之间进行分配和同步, 增强了对网络攻击和系统故障的抵御能力. 通过在不同地域部署备份和冗余系统, 异构云基础设施层能够在自然灾害、硬件故障或其他灾难性事件中快速恢复服务.

网络韧性使能层: 构建韧性核心能力中台, 实现智能感知与动态调控. 该层由安全态势收集器、安全分析引擎、意图分析引擎、韧性控制器等核心模块构成. 安全分析引擎基于多源数据融合, 实现了对安全威胁的细致、多角度、实时的动态分析, 能够精准识别潜在风险, 并配合韧性控制器实施故障隔离、重配置、动态轮换等策略, 防止局部故障扩散至整个网络, 从而在复杂多变的网络环境下保持稳定运行. 此外, 网络韧性使能层还借助 AI 赋能的动态闭环机制, 从预测、防御、检测和响应 4 个方面增强网络韧性.

• 安全态势收集器 (security data collector, SDC): 是一种监控和分析工具, 用于收集网络各种安全相关的数据和信息, 包括网络状态、流量、日志、系统漏洞等数据.

• 安全分析引擎 (security analysis engine, SAE): 接收安全态势收集器收集的数据, 利用分析算法和模型, 以评估和衡量网络安全状态或态势.

• 意图分析引擎 (intent-based analysis engine, IBAE): 识别用户需求或当前网络状态, 将用户需求转换成具体的意图元组, 其中包括网络拓扑、安全策略.

• 韧性控制器 (resilience controller, RC): 根据用户的安全需求, 实施拟态防御、移动目标迁移、容灾备份、安全隔离、负载均衡等安全策略, 然后把任务下发到编排器中.

• 安全编排器 (security orchestrator, SO): 基于标准的 ETSI NFV 架构, 负责 VNF 的生命周期管理和跨云协同管理, 接收韧性控制器的任务, 负责新建一个子网络实例.

• VNF 超市 (VNF supermarket, VNFS): 负责各种不同虚拟化网络功能的管理. VNF 超市是一个开放的空间, 任何符合条件的厂家都可以将自己的网络能力发布到里面, VNF 超市为不同的网络需求打包满足条件的 VNF 模版列表.

• 异构分析引擎 (heterogeneous analysis engine, HAE): 异构分析引擎则负责对同种功能不同厂商的网络组件异构度进行分析, 为冗余方案提供可靠性最大的组件集合.

• 信任评估器 (trust assessor, TA): 是指对网元执行体的信任度进行评估, 包括动态和静态评估,

表 1　参考架构中使能器提供的网络韧性能力对照表.

Table 1　Capability mapping table of cyber resilience enablers in the reference architecture.

Resilience enabler	Capabilities				Objectives			
	MP	DR	PU	FI	PIO	PFT	RRR	SASE
SDC	√	–	–	–	√	–	–	–
SAE	√	–	√	–	√	–	–	–
IBAE	–	√	√	–	–	–	–	√
RC	–	√	–	–	–	√	–	–
SO	–	√	–	√	√	–	√	–
VNFS	–	–	–	√	–	√	–	–
HAE	√	–	–	–	–	√	–	–
TA	√	–	–	–	√	–	–	–

静态评估从代码程序错误、安全热点、漏洞、异味代码数、代码重复率、覆盖率等指标进行度量; 动态评估是依据网元执行体历史运行数据进行评估.

韧性网络功能层: 基于韧性使能层驱动, 构建高度灵活且可编程的定制化网络服务, 并确保网络在复杂多变的环境中保持稳态运行. 6G 网络功能层通过分布式连接功能、智能感知与决策功能、动态修复与迭代更新功能的深度融合, 实现了多要素的一体化调度和管理, 这些功能的协同将为 6G 新业务、新应用提供强大的安全支持, 且满足不同用户的差异化安全需求. 图 3 网络功能层给出了一个内生安全的子网实例, 该子网络具备拟态防御能力, 通过韧性控制器从等价功能异构执行体仓库不断更新等价功能异构执行体, 并基于消息分发代理和拟态输出裁决器实现网元内部消息的分发和裁决, 从而确保网络的高可靠运行.

• 网元执行体 (network function executor, NFE): 指具备某一种网络功能 (如接入和移动性管理功能 (access and mobility management function, AMF) 统一数据管理 (unified data management, UDM)) 的软件实例, 网元执行体通常以 VNF 的形式运行在云基础环境中, 其包含 3 个要素: 底层硬件环境、操作系统、网络功能服务.

• 等价功能异构执行体 (equivalent function heterogeneous executor, EFHE): 指提供同等网络功能服务但实现方式、运行环境存在差异的执行体集合. 可通过对功能上等效的异构代码、同源代码进行构建, 并使用多样性编译器来构建等效的异构执行体, 以此生成不同功能副本. 也可通过将同种网络功能的执行体运行在不同的虚拟环境来实现异构性.

• 等价功能异构执行体仓库 (equivalent function heterogeneous executor pool, EFHEP): 存储了具有功能等价的异构执行体, 等价功能异构执行体根据工作状态分为工作集和非工作集.

• 消息分发代理 (message dispatch agent, MDA): 根据负反馈控制器的策略调度指令决定将外部输入与当前服务集内的指定执行体建立连接, 以实现执行体激活、执行体挂起修复或者执行其他给定的任务, 实现输入消息的动态复制分发, 将收到的消息复制分发给多个等价功能异构执行体进行处理.

• 拟态输出裁决器 (mimic decision point, MDP): 以多个等价功能异构执行体的输出为输入, 依据安全等级, 基于裁决策略 (裁决策略包括多数、一致性等策略) 对同一个输入消息的多个响应结果进行裁决, 以保证输出数据的安全性.

在上述参考架构中, 网络韧性使能层作为核心枢纽, 其各个使能器的设计与实现与第 2 节提出的韧性体系构想能力紧密契合. 具体的对应关系如表 1 所示. 这些使能器分别承载着不同的功能, 通过精准对接韧性体系构想中的各项能力与目标需求, 实现了从理论构想到实际应用的高效转化. 例如, 安全态势收集器对应于韧性体系中的关键能力 —— 多维感知; 而意图分析引擎则赋能韧性体系中的核心目标 —— 自适应与自演化. 这种一一对应的关系不仅确保了使能层各使能器的功能与韧性体系

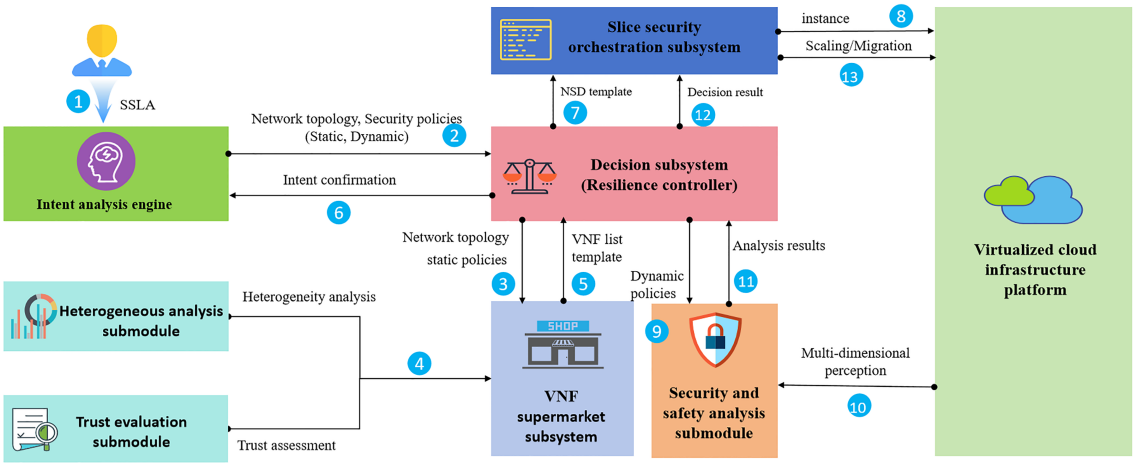

图 4　(网络版彩图) 6G 网络韧性参考架构工作机理.

Figure 4　(Color online) Mechanism of the 6G cyber resilient reference architecture.

构想高度契合, 还为整个网络系统的韧性化、智能化发展提供一定支撑.

3.2　参考架构工作流程

6G 网络韧性参考架构如图 4 所示, 其核心包括意图分析、智能决策、资源编排、动态监控 4 个环节.

在意图分析阶段, 意图分析引擎通过自然语言处理技术对用户输入的模糊安全需求进行语义解析, 将其转化为包含具体网络拓扑参数和安全策略要求的结构化意图元组, 并传输至决策子系统, 决策子系统可以包含韧性控制器的功能, 实现决策和控制的一体化.

在智能决策阶段, 决策子系统接收到需求后, 首先向 VNF 超市子系统发起 VNF 列表模板请求. VNF 超市子根据静态安全策略要求, 协同两大分析模块进行模板匹配: (1) 通过异构分析子模块提供的设备异构度指数, 确保 VNF 链的多样性防御能力; (2) 依托信任评估子模块的代码安全评级, 构建可信 VNF 供应链. 当出现完全匹配空缺时, 采用近似匹配算法返回最优候选方案并附加差异说明. 完成资源遴选后, 决策子系统启动意图验证机制, 通过策略冲突检测引擎进行多维校验, 包括但不限于资源冲突检测、策略叠加冲突校验等, 并采用基于强化学习的冲突消解算法进行自动优化.

在资源编排阶段, 验证通过的 VNF 模板将被封装为标准化网络切片模板, 同步触发两个关键流程: 一方面将切片模板推送至 VNF 编排器子系统启动实例化部署; 另一方面根据动态安全策略生成自适应安全规则集, 注入安全分析引擎构建主动防御能力.

在动态监控阶段, 安全分析引擎基于流式数据处理架构, 实时采集切片运行时的网络流量、资源负载等监控数据, 通过威胁建模和异常检测算法进行持续安全态势评估. 评估结果经决策子系统的事件响应引擎处理后, 生成包括弹性扩缩容、服务迁移等在内的动态防护指令, 形成 “感知 – 决策 – 执行” 的闭环控制机制. 编排器子系统接收指令后, 通过 Kubernetes 等编排工具执行细粒度资源调度, 确保网络安全服务始终维持最优运行状态.

该架构通过结合静态策略与动态响应的双重保障机制, 显著提升了网络防御系统的自适应能力和服务连续性. 为了更清晰地展示上述工作机理中各环节的具体操作步骤, 表 2 详细列出了整个架构运行过程中的关键算法步骤. 这些步骤涵盖了从用户需求解析到资源调度执行的完整流程, 为架构的高效运行提供指导.

以一个拟态切片构造为例, 意图驱动、安全分析引擎以及 DHR 控制器均以服务的形式部署于韧性使能层, 并借助服务化接口与 MANO 或 NFVO 实现通信交互. 当用户提出切片安全部署请求时,

表 2　网络韧性参考架构关键算法步骤.

Table 2　Key algorithm steps in the cyber resilience reference architecture.

Step	Description
1	Parse security requirements and generate intent tuple $I = \langle D, A, O, Ac, R\rangle$
2	Determine orchestration parameters $(T, S) = \text{Determine}(O, Ac)$
3	Obtain required resources $M = \text{GetResources}(T, S)$
4	Select VNF combination $V = \text{SelectVNF}(H, P_s)$ (H: heterogeneity index; P_s: safety level)
5	Return VNF template list $\text{Return}(V)$
6	Confirm intent $\text{Confirm}(I)$
7	Submit NSD template $\text{Submit}(M)$
8	Instantiate slice $I' = \text{Instantiate}(M)$
9	Send dynamic policy $\text{Send}(Ds)$
10	Collect data $Data = \text{Collect}(C, S_s, M_m, Cpu, Traffic, Ps, SysLog, AppLog)$
11	Analyze data $R = \text{Analyze}(Data)$
12	Send security strategy $\text{Send}(S_s)$
13	Execute operation $\text{Execute}(S_s)$

意图驱动模块率先对用户语义展开细致分析, 进而生成包含安全策略、网络拓扑与网络配置等关键要素的意图元组. 基于此意图元组, 决策子系统与 VNFM 模块进行交互协同, 完成 TOSCA 模板的生成工作, 随后将切片模板下发至编排器. 编排器新建一个拟态域网络切片, 并在虚拟资源上生成多个 NFs, 这些 NFs 涵盖了 VNF 的异构副本以及网络功能级的拟态裁决器. 在此过程中, SDN 控制器全力协助, 依据既定安全要求, 实现这些 NFs 的链路连接构建、路由规则下发以及自动化部署等关键操作, 并最终将网络切片已成功生成的相关信息反馈给拟态控制器. 拟态网络切片具备独特的安全运行机制, 其会按照设定的时间周期, 对网元执行体副本进行规律轮换操作, 以此有效迷惑潜在攻击者, 提升网络安全. 而且, 当拟态裁决器感知到执行体遭受攻击时, 会即刻向拟态控制器发出通知. 拟态控制器接收到通知后, 迅速对受攻击的执行体实施清洗与轮换处理. 即便出现单个执行体被攻破的极端情况, 凭借完备的冗余机制, 也能够成功避免因单点故障而引发业务停滞的严重后果, 从而确保网络切片的系统运行韧性.

良好的兼容性使得该架构能够灵活集成现有的先进技术和模型, 提升整体的防御能力. 如在静态安全策略构建中, 通过异构分析子模块和信任评估子模块协同工作, 能够兼容现有的机器学习运维 (machine learning operations, MLOps)、威胁共享平台等安全技术, 为拟态 VNF 的构建提供多维度的安全信息参考. 在动态安全策略方面, 架构所采用的威胁建模和异常检测算法能够与现有的入侵检测系统、入侵防御系统进行深度融合, 进一步提升安全态势感知的精准度. 此外, 基于强化学习的冲突消解算法不仅能够优化内部策略冲突, 还能够与外部的智能优化模型进行协同工作, 实现更高效的资源调度和策略调整.

3.3　韧性能力定性分析

基于提出的智能韧性网络参考架构, 我们构建了两个核心网实例 (实例视频详见文献 [26]), 并与传统方法构建的核心网实例进行了对比, 对比维度涵盖冗余性、弹性扩缩、恢复策略、安全防护 4 个核心方面, 以衡量构建的网络韧性能力.

实例 1 基于参考架构通过意图驱动生成具备拟态防御能力的内生安全核心网切片, 该切片实现了对 UDM 网元的拟态化, 包括新增冗余机制、动态调度、大数裁决机制, 使其能够灵活适应不断变化的网络环境, 具备网元故障或半故障下业务持续性保证能力以及抵抗未知漏洞攻击的能力. 如表 3 所示, 与传统方案相比, 构建的拟态防御核心网切片通过异构冗余、动态策略和内生安全机制, 实现了主

表 3　拟态核心网和非拟态核心网能力对比.

Table 3　Comparison of mimic 5G core and no-mimic 5G core.

Item	Sub-item	Mimic 5G core	No-mimic 5G core
Redundancy method	Redundancy	3 or more	2
	Heterogeneity	High	Low
Defend strategy	Configuration	Dynamic	Static
	Failover	Scheduling	Active-standby
Security method	Security paradigm	Endogenous	Overlay
	Protection target	Unknown vulnerabilities	Known vulnerabilities

表 4　基于 MPDS 的网元扩缩方法和云原生扩缩方法对比.

Table 4　Comparison between MPDS-based and cloud-native scaling methods.

Item	Sub-item	MPDS-based	Cloud-native
Elastic method	Trigger mechanism	Prediction-based	Threshold-based
	Decision-making basis	Multi-dimensional	Single-indicator
Defend strategy	Configuration	Dynamically	Static
	Closed-loop	√	×
Security method	Security paradigm	Proactive	Passive
	High availability	High	Low

动防御和实时抗攻击能力, 提升了系统韧性.

实例 2 基于参考架构生成具备自动缩放能力的核心网切片. 该自动缩放能力基于 MDPS (监控 – 预测 – 决策 – 执行) 模式, 通过 “监控 – 预测 – 决策 – 扩缩执行” 的循环, 实现了 4 个主要阶段的闭环控制. 该方法利用多维度指标进行更精细的决策, 并借助智能算法进行实时预测, 从而提前主动进行扩缩容操作, 显著提升了系统的灵活性和适应性. 如表 4 所示, 传统的云原生扩缩容方法存在被动响应、单一指标依赖以及缺乏预测反馈等问题, 在应对复杂网络环境和安全威胁时往往显得力不从心. 相比之下, 基于智能韧性参考架构生成的方法能够更有效地减轻突发流量的影响, 确保业务的高稳态运行, 展现出更强的系统韧性.

通过两个实例的对比分析, 清晰地展现了所提出的参考架构在提升网络韧性方面的显著优势. 无论是在冗余设计、弹性扩缩容能力、动态策略调整、监控与预测精度, 还是安全防护机制等核心维度上, 基于该参考架构构建的网络实例均展现出系统内生的韧性.

鉴于网络韧性需平衡性能与成本, 且各行业、用户韧性需求各异, 差异化韧性设计必不可少. 以 DHR 架构为例, 一方面, 可构建多级拟态安全体系, 逐级增强功能复杂度与安全性. 如一级在基本服务架构上增加异构备份执行体, 二级则引入负反馈单元. 另一方面, 借助 SDN, NFV 等技术灵活配置资源, 低负载时关闭部分资源或降能耗, 高峰时快速扩展资源保障性能. 同时, 运用 AI 技术实现智能运维, 包括故障预测、诊断、修复, 降低人工运维及故障成本, 提高运营效率, 使网络韧性技术兼顾经济可行性.

4　韧性使能关键技术

为构建 6G 核心网韧性体系, 本文从架构支撑和安全赋能两个维度出发, 给出了潜在的使能关键技术, 进一步对所述技术的作用机理及应用挑战进行简要阐述, 以此为业界韧性架构设计提供参考.

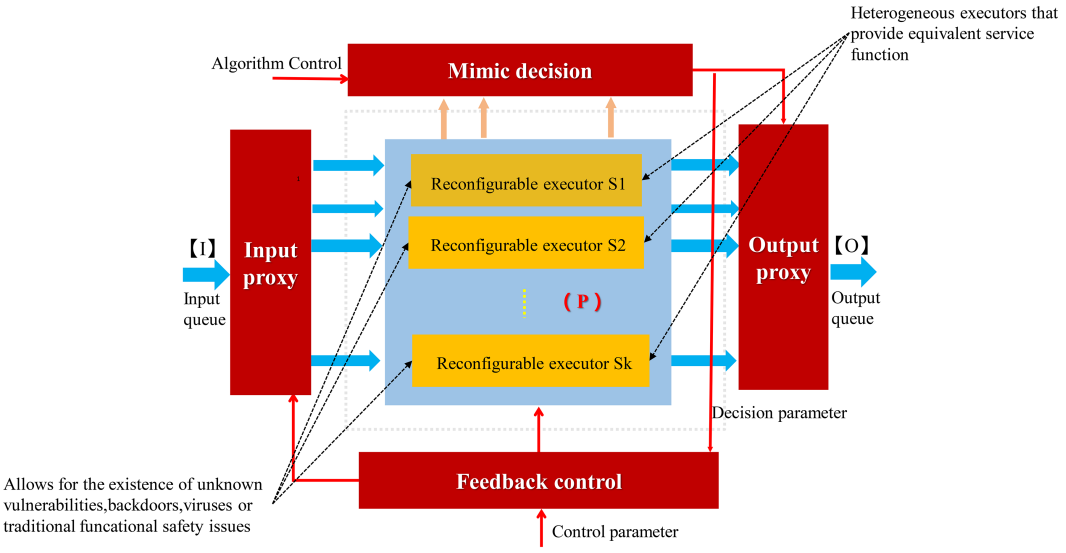

图 5　(网络版彩图) DHR 构造架构图.

Figure 5　(Color online) Diagram of dynamic heterogeneous redundancy architecture (DHR).

4.1　架构支撑类技术

4.1.1　DHR 技术

DHR 技术是一种基于架构级冗余的动态防御体系, 如图 5 所示, 包含输入代理、功能等价异构执行体集合、策略裁决、输出选择和反馈控制, 其核心机理是通过异构性、动态性和冗余性三要素的协同作用提升系统韧性. 该技术通过构建硬件架构、操作系统、通信协议等维度的异构资源池, 结合运行时动态调度机制, 形成具有差异化的冗余执行体. 基于多模裁决机制对异构执行体的输出进行实时验证, 将攻击行为转化为系统内部的差模信号, 从而在未知威胁环境下实现内生安全防护.

将该技术应用于 6G 核心网, 其异构性通过使用多设备、多系统、多网络的复杂性来改变现有业务系统的相似性、单一性, 减少了 6G 网元设备因同种漏洞攻击导致服务不可用概率; 其冗余性减少了网络功能因不可靠或自然灾害导致的服务不可用; 裁决机制利用多模输出比对与异常行为分析, 能够早期检测攻击行为并实时切换到可信的服务实例, 从而保障业务连续性, 同时也能减少网络信息或数据被篡改的风险. 文献 [27] 基于 6G 空天地一体化场景, 给出了内生安全云平台架构, 该框架能自动化地为 6G 核心网微服务提供拟态基础能力, 包括拟态架构编排、异构执行体的选择、定时执行体轮换机制、受攻击执行体轮换机制等. 文献 [28] 将 DHR 应用于 6G 云网融合场景下的服务功能链构造, 并对其韧性能力进行评估, 为 DHR 技术在复杂多变的 6G 云网融合环境中的应用提供了重要的参考和验证.

为适应 6G 核心网演进特征, DHR 技术需要在以下几个方面进行适配和优化, 在时延敏感或高吞吐量场景中, 通过软硬件协同设计等方法, 提高裁决效率; 研究破坏攻击路径和攻击链条的内生安全轻量化构造方法, 以最小的异构代价提供较强的鲁棒性和安全性; 研究利用经验数据训练生成式人工智能, 使其能够根据不同的系统约束和多目标功能/性能属性自动生成内生安全架构所需的异构执行体.

4.1.2　ZSM 技术

零接触网络管理 (zero-touch network and service management, ZSM) 技术旨在实现端到端网络及服务的全自动化管理, 通过构建覆盖网络配置、服务编排、故障修复的全流程自动化框架, 结合 AI/ML 驱动的实时决策与预测能力, 形成自配置、自修复、自优化的闭环管理系统. 文献 [29] 介绍了一种去中心化的零接触式管理框架, 并通过典型用例 (切片级资源预测) 来展示 6G 网络切片大规模部署场

景下的效果. 在跨域的多域网络中, 零接触式管理技术可实现网络切片的跨域创建、配置和资源分配, 确保不同域之间的网络切片的一致性和协同工作能力, 文献 [30] 给出了 ACROSS 项目设计和实现的下一代网络和服务的端到端服务部署和管理平台, 该平台通过多域编排器、深度端到端遥测、人工智能驱动的智能等技术, 实现了跨域的零接触式配置和管理.

面向 6G 开放异构的网络环境, ZSM 搭载零接触式闭环控制技术的自动化和智能化降低人工干预依赖, 减少因配置错误或策略滞后导致的服务中断风险. 通过基于多维感知与动态反馈机制, 快速识别网络异常并触发自适应恢复策略, 将外部扰动转化为系统内部的动态调节信号, 提升网络的动态修复和自我优化能力. 同时对于攻击造成的故障和性能下降, 零接触闭环控制系统能够根据系统状况动态及时灵活调配系统资源, 以保证关键服务正常运行. 为适应 6G 网络超高可靠、超低时延及全域智能的需求, ZSM 技术需在 6G 空天地网络和现有制式网络融合架构的全域业务编排 [31]、高实时性闭环控制增强、生成式 AI 驱动的自主进化等方向深化研究.

4.1.3　零信任技术

零信任是一种以 “永不信任、始终验证” 为核心原则的安全架构. 零信任网络架构认为所有的网络流量都应被视为潜在的威胁, 并需要基于访问主体的身份、网络环境、终端状态等尽可能多的信任要素对所有用户进行持续验证和动态授权. 此外, 区别于传统粗放式授权机制, 零信任通过将访问权限精确限定在应用级、功能级和数据级, 仅向访问主体开放必要的最小化资源集合, 从而有效收缩了潜在攻击面.

面向 6G 核心网全服务化解耦后的复杂攻击挑战, 零信任架构通过三方面机制实现安全防护升级: 其一, 基于动态信任评估引擎, 整合身份可信度、环境风险值、行为合规性等多维度指标, 构建实时动态更新的信任评分模型, 实现网元访问权限的智能调适, 有效遏制恶意网元发起的隐蔽攻击; 其二, 建立协议规范驱动的网元状态机模型, 通过输入种子生成理论行为链, 实时比对实际运行状态与预期轨迹的偏差度, 精准识别异常服务调用模式, 及时阻断异常微服务间的非法交互; 其三, 实施微隔离纵深防御策略, 将 6G 核心网被划分为多个小而隔离的区域, 每个区域都有独立的安全策略和访问控制措施. 这种网络微分段技术有效限制了攻击者在网络内部的横向渗透能力, 即使单点防御失效, 也能通过安全域间的逻辑隔离大幅降低系统性安全风险. 针对 6G 网络泛在接入的愿景, 还需重点突破跨域信任建模关键技术, 研究构建地面移动网与卫星通信网间、运营商基础设施与第三方服务节点间以及多利益主体间的动态信任评估框架, 促进不同网络和服务之间的韧性协作.

4.1.4　网络数字孪生技术

网络数字孪生技术通过集成物理模型、传感器数据和历史运行数据, 创建实体装备的虚拟映射, 反映其全生命周期, 其核心机理基于 “数据 – 模型 – 映射 – 交互” 四要素闭环体系, 依托高保真仿真引擎与实时数据同步机制, 支持对 6G 核心网的全生命周期分析、威胁推演及韧性策略优化. 数字孪生网络 (digital twin networks, DTNs) 在 6G 网络设计、诊断、仿真、假设分析以及 AI/ML 驱动的实时优化与控制等方面发挥重要作用, 文献 [32] 详细介绍了 DTNs 在 6G 的关键应用场景, 包括网络仿真与规划、运营与管理、仿真数据生成、AI 训练与推理等, 并分析了这些场景下的具体需求, 如可靠性、可扩展性、敏捷性等; 最后, 通过 Omniverse 平台上的实际案例展示了 DTNs 的构建与运营, 并对未来的研究方向进行了展望, 包括 AI 与 DTNs 的深度融合、安全与隐私保护机制, 以及标准与行业协调等方面.

该技术可在多个维度为 6G 核心网提供防护: 通过在虚拟空间中创建网络的精确映射, 模拟攻击和数据流转, 预测潜在风险, 测试防御策略, 从而在不影响实际网络的情况下提前识别和防御 APT 攻击, 同时亦可监控和预防隐私数据泄露; 通过建立物理网络的数字映射, 实现对网络动态变化的实时监控, 使网络可以在实际发生故障前预测并准备相应的容错措施, 增强网络的抵抗能力和故障容错性. 此外, 还允许在虚拟环境中测试和验证新的网络策略, 然后将其实施到实际的物理网络中, 使网络能

表 5　架构类技术与 6G 网络韧性能力映射表.

Table 5　Mapping of architectural technologies to 6G network resilience capabilities.

Technology	Threats			Defense			Capabilities				Objectives			
	APT	FT	PL	Point	Line	Plane	MP	FI	DR	PU	PIO	PTF	RRR	SASE
DHR	√	√	√	√	–	√	–	–	√	√	–	√	√	–
ZSM	–	√	–	√	–	√	√	–	√	√	√	–	√	√
ZT	√	–	√	√	–	√	√	√	–	√	–	√	√	√
DTN	√	–	√	√	√	√	√	–	√	√	√	–	–	√

够自适应地响应外部环境的变化. 当前业界对于其与 6G 网络的研究仍处于初级阶段, 在基础技术层需突破多模态数据安全采集、网络威胁数字化建模、跨域攻防知识图谱构建等关键技术; 在系统架构层亟待开展数字孪生体系与 6G 核心网架构的一体化设计.

表 5 给出了各架构类技术与 6G 核心网韧性能力的对照表. 优良的系统架构能够确保网络系统适时感知威胁风险、稳健抵抗威胁攻击、控制威胁在最小范围内、及时应对化解系统扰动并在可接受时间内恢复其功能, 并根据威胁变化智能调整适应的能力.

4.2　能力类技术

4.2.1　AI Agent 技术

AI Agent 技术是一种先进的人工智能系统, 能够在极少的人工指导下执行复杂任务并做出决策. 与传统的自动化工具不同, AI Agent 具备独立思考、适应环境和自主执行任务的能力. 它们通过感知外部环境、分析数据并根据预设目标进行决策, 展现出强大的灵活性和智能性. 文献 [33] 提出了一种在 6G 网络中结合代理工作流与 RAG 的新型框架, 旨在实现更可靠的生成式人工智能. 该框架通过部署能够反思输出并利用外部实时知识的自主代理来提升响应质量和准确性. 文献 [34] 提出了一种新型的 6G 架构, 通过分离控制平面和用户平面, 利用代理 AI 实现服务的无缝扩展和管理. 这种架构简化了网络操作, 提高了服务部署的效率. 自主认知代理通过去中心化决策提高了网络的适应性和弹性.

在 6G 网络中, AI Agent 通过自动化安全防御和智能故障预测与恢复来抵御网络威胁和功能威胁. 对于网络安全威胁, AI Agent 能够实时分析网络流量和行为模式, 主动识别并响应潜在的攻击, 并通过持续学习新的攻击手段动态调整安全策略, 以保持其防御机制的有效性. 针对功能威胁, AI Agent 利用历史数据预测设备故障和服务中断, 提前采取措施, 如重新配置路由路径或激活备用资源, 从而减少服务中断时间并维持高质量的服务. 多个 AI Agent 能够根据环境反馈和历史数据独立进行推理与决策优化, 并在不同地理区域或网络节点间共享信息、协调资源分配及故障恢复策略, 从而实现高效的服务质量保障和自动化的网络管理. 然而, 上述机制的稳定运行尚需要确保 AI Agent 的安全性, 包括对潜在攻击的鲁棒性, 在各种操作环境中实现一致的行为等. 此外, 为了满足实时交互的需求, 开发高效且快速的推理方法也是一个重要的研究方向.

4.2.2　可持续的意图管理技术

可持续的意图管理技术 (sustainable intent-based management, SIBN) 是一种创新网络资源管理和配置方法, 融合网络意图与能源效率 [35]. 依靠动态反馈控制和自动化调整机制, 实现网络高度自适应性与快速恢复能力, 可优化网络行为, 让网络自动适应变化、自我修复以及抵御安全威胁, 同时兼顾能源效率, 提升网络韧性和安全性. 还能将安全意图转为具体指令, 促进资源高效利用与动态调整, 借助智能算法在不影响服务质量的情况下寻找最优配置方案, 并持续监控网络状态和性能指标, 及时响应异常, 快速恢复服务, 保障网络高效稳定运行. 文献 [36] 阐述了电信行业从业者借助意图驱动实施自动化, 以达成 E2E 服务目标的举措, 并呈现了与意图冲突管理有关的实验成果. 文献 [37] 提出了一

种融合隐私感知的切片与安全服务编排架构, 创新性地把用户 “隐私意图” 纳入服务等级协议 (service level agreement, SLA). 置身于 6G 环境下, 该架构运用三重策略提升服务信任度级别 (level of trust, LoT), 从而全方位助力网络弹性目标的实现.

可持续的意图管理技术凭借自动化、自适应性及 AI/ML 应用, 有效应对网络威胁与功能失效问题, 其通过在网络各个阶段收集数据进行意图分析, 实现网络威胁的预测、抵御、恢复、自适应闭环控制, 全方位增强 6G 网络韧性, 保障其在复杂环境下的高效稳定运行. 面向 6G 核心网演进需求, 该技术需重点突破多模态意图理解、策略冲突消解、意图可解释性、意图编排等关键技术 [38], 推动 6G 网络向 “语义驱动、自主进化” 方向发展, 构建具有认知智能的韧性网络系统.

4.2.3　DFP 技术

DFP (dynamic function placement, 动态功能放置) 技术 [39] 允许在不同领域 (从最终用户到中心云) 之间灵活部署和迁移网络功能, 以实现服务的差异化和连续编排. DFP 需要跨领域操作, 要求各领域共享资源和 API 以支持服务发现, 并确保不同云实例之间的网络功能能够高效、技术无关地互联互通. DFP 的核心职责包括功能实例的重新定位和运行时上下文的转移, 与 NFV 的生命周期管理的传统功能紧密相关. DFP 和连续体编排在 6G 架构中相辅相成, 两者共同支持 6G 网络提供高可靠性和韧性服务方面的能力.

DFP 基于动态功能部署与智能副本策略, 为 6G 核心网构建去中心化的冗余防护体系, 通过跨网络域实时迁移网络功能实例并设置弹性副本, 有效规避单点故障. 在 6G 以用户为中心的场景中, DFP 通过上下文感知的服务迁移算法和自适应演化架构, 确保极端场景下业务连续性, 使网络能根据终端需求变化实时重构韧性等级. 面向 6G 全服务化需求, DFP 配合意图驱动的服务编排引擎, 允许用户自定义韧性策略并实现跨域防御资源协同调度, 同时依托 AI/ML 构建威胁知识图谱, 实现攻击链的主动预测与动态防御闭环. 面向 6G 核心网的持续演进, DFP 技术需着力攻克以下关键问题: 一是在跨领域协同中, 如何提升资源共享与 API 调用的效率及稳定性; 二是在功能实例管理方面, 如何增强重新定位与上下文转移的高效性、准确性; 三是如何与新兴技术融合实现协同创新, 更好地满足高可靠性和韧性网络服务.

4.2.4　MLOps 技术

MLOps 技术是一种创新的跨学科实践, 它巧妙地融合了机器学习、DevOps (development and operations) 以及数据工程的核心理念与技术. 通过构建一套全面的模型开发、持续集成/持续交付以及监控治理的全生命周期管理体系, MLOps 为云原生架构注入了强大的 AI 驱动能力, 使其能够更加高效地处理复杂的机器学习任务.

MLOps 技术通过机器学习模型对 6G 核心网的实时数据进行分析, 实现故障的预测与快速诊断, 优化资源分配以满足不同服务和应用的需求, 并集成安全功能如入侵检测和异常检测来增强网络的安全性, 从而提升 6G 核心网的韧性 [40]. 面向 6G 核心网演进需求, MLOps 技术在提升 6G 核心网韧性过程中面临数据管理、模型复杂度、实时性能和安全隐私等挑战 [41]. 数据来源的多样化和异构性增加了数据整合与预处理的难度. 机器学习模型的复杂性和多样性, 如强化学习、联邦学习等不同范式, 对模型管理和部署提出了更高要求. 部分 6G 应用对实时性要求极高, 这对模型的训练和推理速度提出了严峻挑战. 此外, MLOps 的集成可能引入新的安全和隐私风险, 如对抗攻击和数据泄露, 需要确保数据和模型的安全性.

4.2.5　MTD 技术

移动目标防御 (moving target defense, MTD) 通过不断变化网络或系统的配置来提升安全性, 使攻击者难以找到稳定的攻击点. MTD 的核心在于增加系统的不可预测性, 通过定期更改关键参数如 IP 地址和端口, 以及采用随机化技术, 让攻击者难以构建有效的攻击策略. 这种防御策略还具备自适

表 6　能力类技术与 6G 网络韧性能力映射表.

Table 6　Mapping of capability-specific technologies to 6G network resilience capabilities.

Technology	Threats			Defense			Capabilities				Objectives			
	APT	FT	PL	Point	Line	Plane	MP	FI	DR	PU	PIO	PTF	RRR	SASE
AI Agent	√	√	–	√	–	√	–	–	√	√	√	–	–	√
MTD	√	√	–	√	–	√	√	–	√	–	–	√	√	√
DFP	√	√	–	√	–	√	√	√	√	–	√	√	√	–
SRv6	–	√	–	–	√	–	√	√	√	–	–	√	√	–
SIBN	√	–	–	√	–	–	√	–	√	–	√	–	√	–
MLOps	–	√	–	√	–	–	–	–	√	–	–	–	√	–

应能力, 能够自动调整防御措施以应对新的威胁. MTD 在设计时注重防御的深度, 通过多层次的变化提高攻击者的攻击成本.

MTD 通过动态改变核心网网络配置, 增加了系统不可预测性及防御深度, 使得攻击者更难识别系统弱点 [42], 以此有效提高 6G 核心网应对开放环境高级持续威胁的能力. 同时, MTD 还具备自适应能力, 能够依据网络安全状态和系统安全状态调整防御策略, 快速隔离受损部分并动态修复与恢复, 减少攻击成功几率、限制攻击者行为, 进而提升 6G 网络的整体韧性. 通过与软件定义边界等零信任框架的融合 [43], MTD 可构建基于动态凭证的细粒度访问控制, 将威胁控制在最小范围, 最小化降低业务影响. 面向 6G 核心网演进需求, 移动目标防御技术需重点突破以下关键问题: 一是要平衡安全性与性能, 在动态变化网络配置以提升安全性的同时, 确保不牺牲 6G 网络的高性能传输和低延迟等关键性能指标, 精准把控变化频率和范围; 二是实现协同与兼容性, 在复杂的核心网架构中, MTD 要与现有及未来新增的网络功能、协议良好协同, 确保在不同网络场景和业务类型下都能兼容, 无缝融入 6G 核心网体系.

4.2.6　SRv6 技术

SRv6 (segment routing over IPv6) 是一种网络技术, 它结合了 Segment routing (SR) 的灵活性和 IPv6 的普遍性, 旨在提高网络的可编程性、可扩展性和效率. SRv6 允许网络运营商通过在数据包的头部插入一系列的 “段” 来定义数据包的路径, 每个段代表网络中的一个指令或操作, 从而实现对数据流的精确控制. SRv6 技术的核心优势在于其三层可编程能力, 可实现灵活的路径控制.

6G 核心网凭借 SRv6 技术, 能够量身定制多路径传输方案 [44], 以契合丰富多样的安全传输需求, 进而增强网络的用户面韧性. 与此同时, SRv6 与信息编码技术相结合, 可有效降低数据丢失或被截获的风险, 显著提升网络数据传输的安全性和可靠性. 除此之外, SRv6 技术通过简化网络协议 [45], 削减了对传统协议的依赖, 从而降低了网络配置与维护的复杂性, 赋予网络更强的灵活性, 进一步提升了 6G 核心网的韧性. 然而, 面向 6G 核心网的演进需求, 仍有诸多方面亟待优化. 需进一步改进路径规划与流量调度算法, 以适应 6G 网络复杂多变的业务需求和拓扑结构; 要加强与软件定义网络 (software-defined networking) 技术的深度融合, 提升网络控制的智能化水平; 要提高多路径传输的协同效率, 优化网络编码技术的结合方式, 保障业务的连续性; 要增强对不同网络条件和需求的自适应能力, 开发更为灵活的路径选择和策略实施机制.

表 6 给出了各能力类技术与 6G 核心网韧性能力的对照表. 能力类技术作为架构类技术的有力补充, 在 6G 网络中发挥着至关重要的作用. 它深入渗透至链路层和功能服务层, 为网络链路和网络服务提供了强大的韧性保障. 通过持续集成尖端的能力类技术, 6G 网络架构可实现更高效、更灵活、更智能的韧性控制.

在 6G 网络架构中, 韧性使能关键技术之间呈现紧密的关联性和显著的协同效应, 共同在不同维

度上为网络韧性提供坚实支撑. 例如, 动态目标防御 (moving target defense, MTD) 与软件定义边界 (software defined perimeter, SDP) 的零信任技术相互协作, 显著增强 SDP 在零信任架构下的防御能力, 进而有效提升 6G 网络的弹性, 使其能够更加灵活地应对各类安全威胁与网络变化 [43]; 此外, 6G 核心网的 NSSF (network slice selection function) 框架在云原生架构中融合智能边缘计算、机器学习运维以及面向 IT 运维的人工智能, 大大提升了 6G 网络的端到端切片安全编排能力 [46]; 数字孪生技术与先进机器学习方法的结合则有效解决了零接触 6G 网络中的攻击检测问题 [47]; DHR 和 AI Agent 技术进行结合, 可以实现智能化裁决和调度, 保障系统韧性的同时降低业务裁决通信的时延.

5　结论与未来展望

6G 网络的发展不仅仅是对速度和连接性的提升, 更重要的是要强化网络的韧性作为一项内在的质量属性. 在 6G 标准化窗口期开展韧性目标与架构设计的协同研究, 不仅能够规避传统 “先建设后修补” 的安全缺陷, 更可为构建原生韧性网络探索提供技术路径.

本文在内生安全赋能网络韧性设计范式指导下, 首先探讨了当前 6G 核心网韧性领域的研究动态及其面临的挑战, 特别关注如何应对 “未知的未知” 攻击威胁, 随后从 “点 – 线 – 面” 3 个维度提出了核心网韧性体系框架, 用于指导核心网的设计. 该框架不仅明确了构建韧性所需的关键能力, 还设定了韧性建设的核心目标. 基于该理论框架, 进一步给出了具有工程可行性的 6G 核心网韧性参考架构, 阐释了其协同工作机制与动态演化原理. 最后, 对潜在关键使能技术韧性赋能机理和应用挑战进行了识别分析.

未来移动信息网络将承载人机物三元融合的重任, 其复杂系统性风险将呈现叠加级联态势, 6G 核心网韧性急需凸显智能、内生、协同等关键特质. 为推动网络韧性在 6G 中成功落地, 需要从以下几个方面着手: (1) 优化韧性设计, 解决成本、复杂性与性能的权衡, 设计出更高效实用的韧性策略; (2) 突破高效人工智能算法的瓶颈, 为网络注入自组织与自适应的能力, 使其能够自主感知环境变化并迅速做出调整, 以维持网络的超稳态运行; (3) 攻克异构组件间的实时通信与协同控制难题, 通过设计标准化接口协议和分布式协调算法, 实现网络组件的韧性联动, 形成 “局部韧性 – 全局稳健” 的协同效应; (4) 完善韧性指标体系, 推动 6G 网络韧性指标标准化, 并开展测量系统韧性的专项研究, 为网络韧性的准确评估与持续提升提供坚实的科学依据.

参考文献

1 Zhang P, Chen Y, Wu C N. Six-generation mobile communication: development trend and outlook. Strategic Study CAE, 2023, 25: 1–8 [张平, 陈岩, 吴超楠. 6G: 新一代移动通信技术发展态势及展望. 中国工程科学, 2023, 25: 1–8]

2 Next G Alliance. Next G Alliance report: roadmap to 6G. 2022. https://nextgalliance.org/white_papers/roadmap-to-6g/

3 SNS JU. SNS Journal 2024. 2024. https://smart-networks.europa.eu/sns-journal-2024/

4 NGMN. 6G trustworthiness considerations. 2023. https://www.ngmn.org

5 Nokia Bell Labs. Security and trust in the 6G era. 2021. https://www.nokia.com/asset/210527

6 NIST. Developing cyber-resilient systems: a systems security engineering approach. 2021. https://doi.org/10.6028/NIST.SP.800-160v2r1

7 Akinsanya M O, Ekechi C C, Okeke C D. The evolution of cyber resilience frameworks in network security: a conceptual analysis. Comput Sci IT Res J, 2024, 5: 926–949

8 Zhu Q Y. Foundations of cyber resilience: the confluence of game, control, and learning theories. 2024. ArXiv:2404.01205

9 Li R, Decocq B, Barros A, et al. Estimating 5G network service resilience against short timescale traffic variation. IEEE Trans Netw Serv Manage, 2023, 20: 2230–2243

10 National Science Foundation (NSF). Resilient intelligent NextG systems (RINGS) (2021-02-25) [2023-10-01]. https://www.nsf.gov/pubs/2021/nsf21052/nsf21052.jsp

11 Open6Ghub. Organic 6G software-based networks: adaptability, flexibility, simplicity, reliability and openness at the system level. 2024. https://www.open6ghub.de

12 NextG Alliance. Trust, security, and resilience for 6G systems. 2022. https://nextgalliance.org/white_papers/trust-security-and-resilience-for-6g-systems/

13 Wu J X. Cyber Resilience System Engineering Empowered by Endogenous Security and Safety. Cham: Springer, 2024. 1–10

14 Wu J X, Ji X S, He L, et al. Cyber resilience enabled by endogenous security and safety: vision, techniques, and strategies. Strategic Study CAE, 2023, 25: 106–115 [邬江兴, 季新生, 贺磊, 等. 内生安全赋能网络弹性研究. 信息通信技术, 2023, 25: 106–115]

15 China Unicom Research Institute. White paper on 6G core network system architecture and key technology prospects. 2024 [中国联通研究院. 6G 核心网系统架构及关键技术展望白皮书. 2024]https://www.vzkoo.com/document/20240905d84e758e19f22d99963923dc.html

16 Duan X D, Wang X Y, Lu L, et al. 6G architecture design: from overall, logical and networking perspective. IEEE Commun Mag, 2023, 61: 158–164

17 China Telecom Research Institute. White paper on 6G network architecture prospects. 2023 [中国电信研究院. 6G 网络架构展望白皮书. 2023]http://doc.cserver.com.cn/doc_df7c6d42-6dc5-48c0-be7b-d7f329c587c1.html

18 Wu J J, Sun L, Wang D H, et al. Endogenous security architecture and key technologies for 6G networks. Sci China Inf Sci, 2024, 54: 2881–2904 [吴建军, 孙黎, 王东晖, 等. 面向 6G 网络的内生安全架构和关键技术思考. 中国科学: 信息科学, 2024, 54: 2881–2904]

19 Yang Z, Chen M, Wong K K, et al. Federated learning for 6G: applications, challenges, and opportunities. Engineering, 2022, 8: 33–41

20 Xie Z C, Zhang M J, Xu L, et al. New requirements and key technologies for 6G network security. Posts Telecommun Design Technol, 2024, 8: 49–52 [谢泽铖, 张曼君, 徐雷, 等. 6G 网络安全新需求及关键技术研究. 邮电设计技术, 2024, 8: 49–52]

21 Tabansky L, Lichterman E. PROGRESS: the sectoral approach to cyber resilience. Int J Inf Secur, 2025, 24: 18

22 Valenza F, Karafili E, Steiner R V, et al. A hybrid threat model for smart systems. IEEE Trans Dependable Secure Comput, 2023, 20: 4403–4417

23 van Acken J, Gadellaa J F, Jansen S, et al. Poster: the unknown unknown: cybersecurity threats of shadow IT in higher education. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, New York, 2023. 3633–3635

24 National Cybersecurity Standardization Technical Committee. Cybersecurity technology—Cyber-resilience evaluation criteria. National Standard GB/T 44862-2024, China, 2024 [全国网络安全标准化技术委员会. 网络安全技术网络弹性评价准则. 国家标准 GB/T 44862-2024, 中国, 2024]https://www.antpedia.com/standard/1792725071-1.html

25 Purple Mountain Laboratory. White paper on network resilience measurement technology based on system architecture evaluation. 2023 [紫金山实验室. 基于系统架构评估的网络弹性度量技术白皮书. 2023]https://www.sgpjbg.com/baogao/113220.html

26 czypml. 6GCoreNetwork. GitHub. https://github.com/czypml/6GCoreNetwork

27 Ji X S, Huang K Z, Wu J X, et al. Endogenous security for the space-integrated-ground information network in 6G. Space-integrated-ground information networks, 2023, 4: 2–12 [季新生, 黄开枝, 邬江兴, 等. 6G 天地一体化信息网络内生安全技术. 天地一体化信息网络, 2023, 4: 2–12]

28 Zhou D, Ji X, You W, et al. TCPN-based resilience evaluation of SFC with dynamic heterogeneous redundant structure towards 6G networks. In: Proceedings of the 10th International Conference on Computer and Communications (ICCC), Chengdu, 2024. 2253–2259

29 Chergui H, Ksentini A, Blanco L, et al. Toward zero-touch management and orchestration of massive deployment of network slices in 6G. IEEE Wireless Commun, 2022, 29: 86–93

30 Giannopoulos D, Katsikas G, Trantzas K, et al. ACROSS: automated zero-touch cross-layer provisioning framework for 5G and beyond vertical services. In: Proceedings of Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, 2023. 735–740

31 Ouyang Y, Zhang Y Q, Ye X Z, et al. White paper on 6G OSS technology. 2023 [欧阳晔, 张亚勤, 叶晓舟, 等. 6G OSS 技术白皮书. 2023] https://arxiv.org/pdf/2307.09045

32 Lin X, Kundu L, Dick C, et al. 6G digital twin networks: from theory to practice. IEEE Commun Mag, 2023, 61: 72–78

33 Ale L, King S A, Zhang N, et al. Enhancing generative AI reliability via agentic AI in 6G-enabled edge computing.

Nat Rev Electr Eng, 2025, 2: 441–443
34 Zhang R C, Tang S P, Liu Y Q, et al. Toward agentic AI: generative information retrieval inspired intelligent communications and networking. 2025. ArXiv:2502.16866
35 Mekrache A, Ksentini A, Verikoukis C. Intent-based management of next-generation networks: an LLM-centric approach. IEEE Netw, 2024, 38: 29–36
36 Alemany P, Muñoz R, Cisneros J C, et al. Defining intent-based service management automation for 6G multi-stakeholders scenarios. IEEE Open J Commun Soc, 2025, 6: 2373–2396
37 Alonso-Lupez J A, Hernández L A M, Arteaga S P, et al. Level of trust and privacy management in 6G intent-based networks for vertical scenarios. In: Proceedings of the 1st International Conference on 6G Networking (6GNet), Paris, 2022. 1–4
38 Ojaghi B, Vilalta R, Muñoz R. Intent-based network resource slicing in 6G. In: Proceedings of the 15th International Conference on Network of the Future (NoF), Castelldefels, 2024. 31–37
39 HEXA-X. Initial 6G architectural components and enablers. (2021-12-31) [2023-09-15]. https://hexa-x.eu/wp-content/uploads/2022/01/Hexa-X_D5.1_full_version_v1.0.pdf
40 Rezazadeh F, Chergui H, Alonso L, et al. SliceOps: explainable MLOps for streamlined automation-native 6G networks. IEEE Wireless Commun, 2024, 31: 224–230
41 Li P, Mavromatis I, Farnham T, et al. Adapting MLOps for diverse in-network intelligence in 6G era: challenges and solutions. 2024. ArXiv:2410.18793
42 Soussi W, Christopoulou M, Xilouris G, et al. Moving target defense as a proactive defense element for beyond 5G. IEEE Comm Stand Mag, 2021, 5: 72–79
43 Abdelhay Z, Bello Y, Refaey A. Toward zero-trust 6GC: a software defined perimeter approach with dynamic moving target defense mechanism. IEEE Wireless Commun, 2024, 31: 74–80
44 Zhao Y, Liao X, You W, et al. CMT-SRv6: a customizable multipath transmission scheme for 6G edge network. IEEE Sens J, 2024, 24: 42138–42151
45 Mo Z, Long B. An overview of SRv6 standardization and application towards 5G-advanced and 6G. In: Proceedings of IEEE 5th International Conference on Computer and Communication Engineering Technology (CCET), Beijing, 2022. 266–270
46 Silva D D C, Sousa M A F D, Oliveira W D, et al. NSSF function in 6G networks based on MLOps deployment model. In: Proceedings of the 27th International Symposium on Wireless Personal Multimedia Communications (WPMC), Greater Noida, 2024. 1–6
47 Bolat-Akça B, Bozkaya-Aras E, Canberk B, et al. An intelligent digital twin model for attack detection in zero-touch 6G networks. In: Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops), Denver, 2024. 773–778

6GC cyber resilience: vision, architecture, and key technologies

Xinsheng JI[1,2], Xingxing LIAO[2*], Jie YANG[1], Wei YOU[1], Zilong WANG[3], Cong LI[3], Hang QIU[1] & Runhan FENG[2]

1. *National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China*
2. *Purple Mountain Laboratories, Nanjing 211111, China*
3. *School of Cyber Engineering, Xidian University, Xi'an 710071, China*
* Corresponding author. E-mail: liaoxingxing@pmlabs.com.cn

Abstract The sixth-generation (6G) mobile communication system is a digital infrastructure supporting the tripartite integration of human, machine, and material society; it exhibits complex characteristics including open heterogeneity, cloud-network convergence, and endogenous intelligence. Cyber resilience, which is a critical intrinsic characteristic of 6G systems, ensures their continuous and reliable operation in complex environments. In this study, we propose a 6G core (6GC) cyber-resilience architecture framework by providing a systematic analysis of the research trends and technological evolution in 6G cyber resilience. In particular, we present a"3-3-4-4-2" paradigm guided by endogenous security and safety principles. The aim of the proposed framework is to address three core challenges: advanced persistent threats in open environments, cloud-based network function failure risks, and cross-domain privacy data leakage. By establishing a three-dimensional "point-line-plane" resilience improvement mechanism, the proposed framework systematically integrates four core capabilities, i.e., multidimensional perception, dynamic remediation, progressive updating, and flexible integration, thereby achieving four resilience objectives. Additionally, we establish a testable and verifiable resilience evaluation system. Building upon this concept, we further propose an engineering-feasible resilience reference architecture for 6G systems by elaborating its collaborative operation mechanisms and dynamic evolution principles. Multiple candidate key technologies are identified, providing both theoretical foundation and technical implementation pathways for constructing 6G networks with endogenous resilience.

Keywords 6G, core network, cyber resilience, collaborative security, assessment framework