

基于形式化推导的 6G 关基安全保护框架设计

Design of Critical Information Infrastructure Security Protection Framework for 6G Based on Formal Derivation

孙翊豪¹, 孔令飞¹, 沈 元² (1. 中国联通河北分公司, 河北 石家庄 050000; 2. 中国联通数据科学与人工智能研究院, 北京, 100000)

Sun Yihao¹, Kong Lingfei¹, Shen Yuan² (1. China Unicom Hebei Branch, Shijiazhuang 050000, China; 2. China Unicom Data Science and Artificial Intelligence Research Institute, Beijing 100000, China)

摘 要:

从电信行业关基合规管理视角审视了5G关基防护体系的底层假设及其在6G场景下可能存在的矛盾, 重构“边界—资产—风险”核心概念, 提出“架构层—资产层—防护层—合规层”一体化保护框架及落地机制。通过攻击树逻辑推演与防御覆盖率集合运算, 从攻击路径阻断、威胁覆盖完备性和响应时效压缩3个维度, 验证了该框架应对跨域代际传导风险与感知复合威胁的理论有效性。

关键词:

6G; 关键信息基础设施; 空天地一体化; 安全保护框架; 代际平滑过渡

doi: 10.12045/j.issn.1007-3043.2026.09.016

文章编号: 1007-3043(2026)09-0084-05

中图分类号: TN918

文献标识码: A

开放科学(资源服务)标识码(OSID):



Abstract:

From the perspective of critical information infrastructure (CII) compliance management in the telecommunications industry, the underlying assumptions of 5G CII protection systems and their potential contradictions in 6G scenarios are systematically examined. The core concepts of "boundary – asset – risk" are reconstructed, and an integrated protection framework covering "architecture layer, asset layer, protection layer, compliance layer" as well as its implementation mechanism are proposed. With attack tree logic deduction and defense coverage set operations adopted, the theoretical effectiveness of the proposed framework in addressing cross-domain intergenerational transmission risks and perceptual composite threats is verified from three dimensions: attack path blocking, full threat coverage, and response time compression.

Keywords:

6G; Critical information infrastructure (CII); Space-air-ground integrated network; Security protection framework; Inter-generational smooth transition

引用格式: 孙翊豪, 孔令飞, 沈元. 基于形式化推导的6G关基安全保护框架设计[J]. 邮电设计技术, 2026(9): 84–88.

1 概述

1.1 背景和挑战

关键信息基础设施(关基)是国家安全与社会运行的重要基础。《关键信息基础设施安全保护条例》^[1]实施以来, 电信行业加快了5G网络安全防护体系的建。但是, 6G的空天地一体化^[2]与通信感知一体化^[3]

正在颠覆该体系的底层假设。结合5G向6G演进的代际连续性判断^[4]与现有组网架构的逻辑推演, 6G与5G将在核心网、骨干链路等设施上长期共存并深度耦合。6G威胁可能经共用基础设施“倒灌”(本文借指跨代风险反向传导)至5G体系。

1.2 研究现状与理论缺口

在国际上, 以3GPP TR 38.821^[5]与ITU-R IMT-2030^[6]为代表, 其本质属于通信安全技术规范^[7], 文献^[8]亦予以旁证。欧美学术研究多集中于通感物理层

收稿日期: 2026-07-17

抗干扰、卫星信道保密^[9]等纯技术算法的优化。总体呈现“重技术轻管理”的特征,较少涉及关基分级防护、资产定级与合规管理体系。国内对关基防护体系的既有研究^[10]对6G资产认定、动态定级和跨域协同应急等管理机制等问题留有空白。

本文发现如下3项理论缺口:边界防护方面目前仍依赖物理隔离,难以适配无固定边界的跨域组网,基于动态信任的逻辑边界管控理论薄弱;技术防护方面未覆盖感知信号伪造等通感复合风险;动态合规方面以静态、属地化的定级、台账和应急机制为主,无法适配资产泛在移动与拓补实时变化。

上述缺口在6G场景中表现为适配矛盾,本文3.2节将以填补这些缺口为理论出发点。

2 5G关基体系现状及其与6G适配矛盾

2.1 5G防护体系概述

现行5G保护体系基于YD/T 4999-2024^[11]构建,其核心网安全架构遵循3GPP TS 33.501^[12]定义的网元间信任模型与安全边界划分原则,具体包括:基于安全域和防火墙的边界隔离,基于线下盘点和属地备案的固定资产分级,以通信加密、入侵检测和漏洞闭环为主的技术防护,依托预案、演练和年度测评的合规应急^[13]。

2.2 5G体系底层假设

固定边界假设网络边界清晰稳定,可实施纵深防御;属地资产假设核心资产固定部署,支持线下核查;单一风险假设风险主要来源于网络攻击和通信数据泄露;静态合规假设拓扑与资产规模相对稳定,可实行年度静态定级和属地应急。

2.3 6G场景系统性适配矛盾

6G特征与上述假设冲突,有失效可能,具体如下。

a) 边界防护结构性失效。空天泛在接入使物理边界模糊,攻击者可绕过地面防线实施跨域渗透。

b) 资产管控体系性失效。低轨卫星、无人机等资产缺乏固定运维点,线下盘点难以实施;现有指标又未覆盖新型资产,造成识别和台账缺位。

c) 技术防护维度能力空白。现有体系缺少感知信号校验、隐私脱敏等模块,难以应对感知欺骗、数据伪造,且重型安全设备不适配空天轻量化节点。

d) 合规应急跨域机制空白。应急预案均为属地单主体模式,难以处置跨空域、跨主体事件,缺乏联合研判与协同处置机制。

3 6G关基保护框架与核心机制设计

3.1 核心概念

安全边界重构。由物理边界转向以“零信任”为理念的全域逻辑信任边界。通过软件定义边界(SDP)^[14]与分布式身份认证,建立贯穿空天地的动态鉴权体系。

关键资产重构。由地面固定资产扩展为泛在动态资产,将低轨卫星、信关站、通感基站及感知数据等新型资产纳入全量资产视图。

安全风险重构。由单一通信风险扩展为“通信—感知—计算”复合风险,开展多维关联分析。

3.2 框架分层设计

如图1所示,框架分层设计参考了业界6G网络架构的分层思想^[15],各层级的功能定位与协同关系如下。

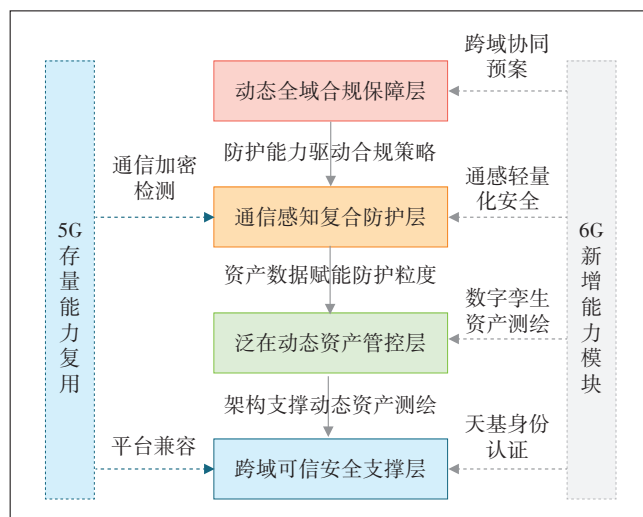


图1 四层一体化6G关基保护框架总体架构示意

a) 架构层(跨域可信安全支撑层)部署分布式身份管理平台与全域态势感知中心,为星地节点提供可信接入、动态鉴权和跨域威胁洞察,破除传统物理边界限制。

b) 资产层(泛在动态资产管控层)利用远程遥测和数字孪生^[16]自动识别、持续监测泛在资产并维护动态台账,建立基于功能、风险、影响的三维动态定级模型。

c) 防护层(通信感知复合防护层)采用“复用+补强”模式,继承5G通信加密和入侵检测能力,增设轻量化节点安全代理、感知信号完整性校验及代际风险隔

离切片。

d) 合规层(动态全域合规保障层)建立覆盖卫星失联、感知数据泄露等场景的跨域跨主体专项预案,明确运营商、卫星企业等主体责任,形成协同应急与问责闭环。

3.3 核心落地机制

落地机制与框架层级、所解决矛盾的对应关系如表1所示。

表1 落地机制与框架层级、所解决矛盾的对应关系

落地机制	对应框架层	解决的核心矛盾
动态资产定级机制	资产层、防护层	资产管控体系性失效
跨域联合应急机制	合规层	合规应急跨域机制空白
多方权责界定机制	合规层	合规应急跨域机制空白
3个阶段平滑过渡机制	全局	代际耦合风险传导(贯穿性矛盾)

3.3.1 动态资产定级机制

建立动态资产关键指数(Dynamic Criticality Index, DCI)模型,量化泛在资产的关键程度。对于任意资产 $a \in A$,其定级函数定义为:

$$DCI(a, t) = \alpha \times C_{base}(a) + \beta \times \Delta E(a, t) + \gamma \times \sum_{i=1}^n R_i(a, t) \quad (1)$$

其中, C_{base} 为基础功能等级(常量), ΔE 为数字孪生实时监测的拓扑连接度变化量, R_i 为当前暴露的威胁风险系数。定级触发条件为 $\left| \frac{dDCI}{dt} \right| > \theta$ 或网络拓扑变更事件 ε 通过该映射,资产等级由静态年度更新转变为事件驱动的实时计算。需要注意的是,资产集合 A 在任意时刻 t 为当前已识别资产的快照闭集。新资产首次进入 A 时,DCI以 $C_{base}(a)$ 为初始值, ΔE 项在首次遥测完成后生效,避免定义域跳变。

DCI机制的完整运行流程如图2所示。DCI的参数标定与收敛阈值需由实测数据校准,本文重点解决其逻辑架构与触发时效的数学表达。本文将数字孪生的实时遥测与状态同步能力^[16]作为DCI的底层使能技术。

3.3.2 跨域联合应急机制

建立贯通卫星、地面等主体的联合指挥平台与专项预案库,明确跨域事件的研判和协同处置流程。

3.3.3 多方权责界定机制

依据《条例》^[1]构建运营商总控、卫星方运维、厂商技术支撑、感知方数据合规的责任矩阵,实现全链路

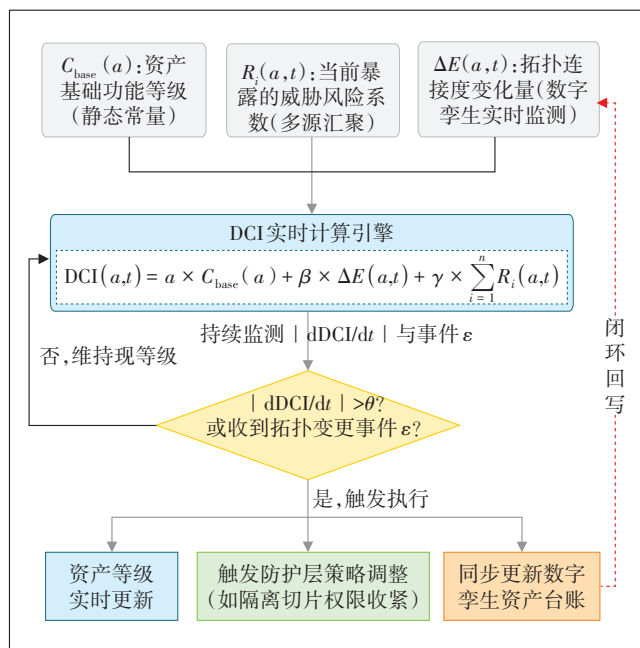


图2 动态资产定级机制(DCI)运行流程

追溯与考核。

3.3.4 3个阶段平滑过渡机制

3个阶段平滑过渡机制包括试点适配阶段、迭代融合阶段和全域落地阶段。

a) 试点适配阶段。在6G试验网与5G核心网之间部署代际隔离切片,阻断新型威胁通过共享链路向现网传导,同时保持业务数据正常互通。

b) 迭代融合阶段。DCI动态定级与统一身份认证逐步上线,DCI监测到风险指数突变时自动收紧跨代权限并触发“熔断”。

c) 全域落地阶段。5G与6G安全策略完成整合,隔离切片淡出,代际安全能力实现一体化运营。该路径保障存量业务不中断、增量风险不扩散。

4 框架有效性推演与形式化评估

本文选择攻击树/攻击图作为推演工具^[17],在缺少真实的6G部署和攻击数据的条件下,该方法可确定性分析防御机制对攻击空间的覆盖完备性。本文仅涉及4个原子条件的逻辑截断,避免状态爆炸问题。

4.1 典型威胁场景构建与攻击图建模

延续场景A(跨域渗透)与场景B(感知伪造)。为评估框架的防御效能,引入防御覆盖率指标 η 。设攻击者所有可能的攻击路径集合为 P_{all} ,被防御机制有效阻断的路径子集为 $P_{blocked}$,则:

$$\eta = \frac{|P_{\text{blocked}}|}{|P_{\text{all}}|} \times 100\% \quad (2)$$

防御机制有效的一个充分条件是:存在一项已部署的防护能力 $\phi \in \Phi$,能够使攻击前提集合 Ψ 中的至少一个必要条件失效。即若攻击者达成最终目标需同时满足 $\Psi_A = \{g_1, g_2, g_3, g_4\}$,则当 $\exists g_i \in \Psi$ 使得 ϕ 直接阻断或永久移除 g_i 时,该攻击路径不成立。

4.2 场景A:跨域渗透的路径阻断逻辑与定级关联

枚举攻击者需顺序满足的原子条件集合 $\Psi_A = \{g_1, g_2, g_3, g_4\}$,分别对应“突破天基认证”“获取星地链路权限”“绕过地面IP隔离”“伪装运维流量”。

传统5G体系 Φ_{5G} 未覆盖天基上下文,导致 Ψ_A 全部条件均满足, $\eta_{5G} = 0\%$ 。在本文框架下,架构层统一身份认证引入了时空约束集合 Y 使得原子条件 g_1 的满足概率被严格归零(逻辑截断)。特别地,DCI的动态性设计可实现主动防御:当卫星节点 α 的DCI因轨道接入突变而实时升高时,自动触发 ε 事件,将代际风险隔离切片的动态权限收紧,直接阻断了 g_2 ,与 g_3 的关联依赖。因此,路径集合 $P_{\text{blocked}} \equiv P_{\text{all}}$,框架在此场景下的覆盖率 $\eta_A = 100\%$ 。图3所示为攻击路径的推演过程。

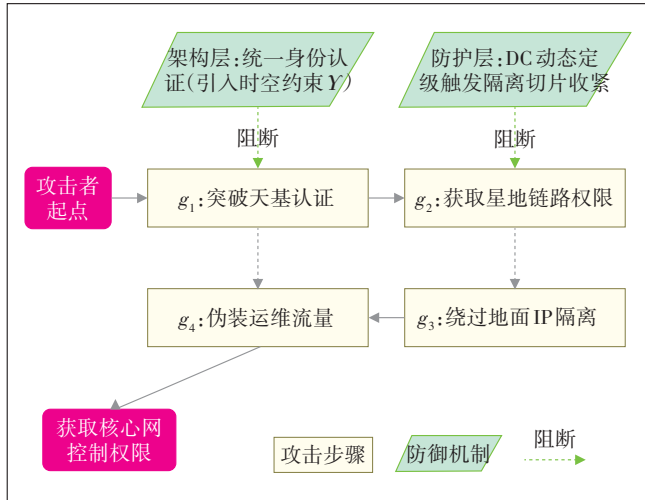


图3 跨域渗透攻击路径推演示意

上述推演假设攻击者严格沿 $g_1 \rightarrow g_2 \rightarrow g_3 \rightarrow g_4$ 路径推进。可进一步考虑如下2种潜在绕过防御的企图。

a) 攻击者尝试跳过 g_1 ,直接从地面网络侧发起渗透。但在本文中,架构层统一身份认证已覆盖全网节点,地面侧同样不构成免认证入口,绕过路径的前提

条件集合与 g_1 等价,同样被时空约束集合 Y 截断。

b) 攻击者尝试篡改DCI的输入参数(如虚报 ΔE 值),使DCI异常降低从而规避隔离切片收紧。该攻击需先获得对数字孪生遥测通道的写入权限,但该通道本身受架构层身份认证保护,构成攻击前提的递归依赖。因此,绕过企图的前提条件集合均为 Ψ_A 或其子集的等价变形,已被 Φ 完全覆盖, $\eta_A = 100\%$ 的结论在绕过场景下依然成立。

4.3 场景B:通感复合威胁的防御完备性

场景B涉及通信与感知2个维度的复合攻击。传统5G体系仅覆盖通信维度的威胁防护(Φ_{5G}),而感知维度形成盲区:攻击者可依次实施“注入伪造感知信号”(h_1)、“篡改环境重建数据”(h_2)、“批量导出用户隐私画像”(h_3),全程可绕过现有安全机制检测, $\eta_{5G} = 0\%$ 。

本文框架在防护层中增设了感知信号完整性校验模块(ϕ_{check})与细粒度数据审计模块(ϕ_{audit}),形成 $\Phi_{\text{new}} = \Phi_{5G} \cup \Phi_{\text{感知}}$ 的防护集合。 ϕ_{check} 在信号接入阶段检测并丢弃伪造的感知波形,使 h_1 的前提条件永不满足; ϕ_{audit} 对数据导出行为实施实时监控,阻断 h_3 。因此,攻击路径集合 P_{all} 被完全覆盖, $\eta_B = 100\%$ 。从集合关系看,复合威胁空间为 $T = T_{\text{通信}} \cup T_{\text{感知}}$ 是 Φ_{new} 的子集($T \subseteq \Phi_{\text{new}}$),防御完备性在理论上恒成立。

4.4 “动态定级与过渡机制”的非攻击图验证

动态定级与过渡机制不直接阻断攻击链,其效能可通过响应时效不等式验证。

设 T_{static} 为传统人工线下定级的响应周期(通常按天计算), T_{dynamic} 为本文DCI函数的计算延迟(毫秒级), $T_{\text{dynamic}} \ll T_{\text{static}}$ 。在攻击窗口内,若攻击在 T_{static} 周期内发生,传统体系存在无防护暴露窗口 $\tau_{\text{expose}} \approx T_{\text{static}}$ 。本文框架通过数学映射将暴露窗口压缩为:

$$\tau_{\text{expose}}^{(\text{new})} = \max \{ \Delta t_{\text{compute}}, \Delta t_{\text{sync}} \} \approx O(1) \quad (3)$$

该不等式在逻辑上严格优于传统模式,且在现代计算条件下,该时间开销可被工程化地控制在毫秒级以下。对于“3个阶段平滑过渡机制”,其作用对象为管理流程而非网络防御,本文将将其定位为框架落地的充分非必要条件,不纳入防御效能量化模型。

4.5 评估结论

本章通过攻击图路径枚举与防御覆盖率集合运算,从数学逻辑上严格证明了本文框架对跨域渗透与通感复合2类典型6G威胁的结构性防御的完备性。

此处“完备性”仅限于对所推演攻击模式的条件全覆盖,并非穷举所有攻击向量。同时,响应时效的逻辑不等式证明消除了传统静态管理固有的暴露窗口。后续工程实测可按需标定参数 α, β, γ 及触发阈值 θ ,与下文5.3节所述实测校准工作衔接。

5 结论与展望

5.1 核心结论

本研究核心结论如下。

a) 现行5G关基防护体系的底层假设与6G动态泛在、通感融合的特征存在本质冲突,面临结构性失效问题。

b) 在重构“安全边界、关键资产、安全风险”概念的基础上提出“架构层—资产层—防护层—合规层”一体化框架,补齐理论缺口。

c) 配套设计动态定级、跨域应急、多方权责与3个阶段过渡机制,为合规落地与代际平滑演进提供可操作性。

5.2 研究局限

本文基于攻击树逻辑推演、防御覆盖率集合运算与响应时效分析,仅在验证方法上提供了理论有效性的充分证据,在6G网络实现前无法进行真实事件数据校准。在研究范畴上,本文聚焦于运营商视角的体系构建与合规管理,并未深入底层安全算法、芯片设计等研发细节。

5.3 未来展望

基于现有成果,后续研究将沿如下路径推进。

a) 探索将AI技术应用于态势感知与动态定级模型,以增强框架的自适应响应能力。

b) 依托6G规模试验网,对本文所提关键机制开展实证验证与参数调优,推动理论模型向实用化工具演进。

c) 立足本框架的实践基础,积极促成行业标准立项,细化资产认定、分级防护及应急处置等关键环节的规范要求。考虑到6G网络的供应链复杂化问题,还将进一步针对全链条安全风险传导与管控,研究并提出治理方案。

参考文献:

[1] 中华人民共和国国务院. 关键信息基础设施安全保护条例(国务院令 第745号) [EB/OL]. (2021-07-30) [2026-06-19]. https://www.gov.cn/gongbao/content/2021/content_5636138.htm.

- [2] IMT-2030(6G)推进组. 6G总体愿景与潜在关键技术白皮书[R]. 北京:IMT-2030(6G)推进组,2021.
- [3] 王诗悦,程凯欣,陈昱帆,等. 通感一体化内生安全威胁及其跨层防御综述[J]. 航空学报,2026,47(11).
- [4] 张平,牛凯,田辉,等. 6G移动通信技术展望[J]. 通信学报,2019,40(1):141-148.
- [5] 3GPP TR 38.821 Solutions for NR to support non-terrestrial networks (NTN) (Release 16.2.0)[S].
- [6] ITU-R. Recommendation ITU-R M.2160-0 Framework and overall objectives of the future development of IMT for 2030 and beyond[R]. Geneva:International Telecommunication Union,2023.
- [7] Saad W, Bennis M, Chen M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems [J]. IEEE Network,2020,34(3):134-142.
- [8] Nguyen V L, Lin P C, Cheng B C, et al. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges [J]. IEEE Communications Surveys & Tutorials,2021,23(4):2384-2428.
- [9] Giordani M, Ardizzone F, Crosara L, et al. The Role of Non-terrestrial Networks: Features and Physical-Layer Security Concerns [M]// Physical-Layer Security for 6G. Hoboken: Wiley,2024:275-303.
- [10] 胡丽娜,蒋凯元,姜静. 关键信息基础设施系统安全防护前沿技术研究[J]. 信息安全研究,2025,11(12):1075-1080.
- [11] YD/T 4999-2024 电信行业关键信息基础设施安全保护 安全管理总体要求[S].
- [12] 3GPP TS 33.501 Security architecture and procedures for 5G System (Release 18)[S].
- [13] 工业和信息化部. 公共互联网网络安全突发事件应急预案:工信部网安[2017]281号[EB/OL]. (2017-11-23) [2026-06-19]. https://www.miit.gov.cn/jgsj/waj/wjfb/art/2017/art_3004ae7575a2458b8080d9fad77911ab.html.
- [14] Rose S, Borchert O, Mitchell S, et al. NIST Special Publication 800-207: Zero Trust Architecture [R]. Gaithersburg: National Institute of Standards and Technology,2020.
- [15] 中国移动通信集团有限公司. 中国移动6G网络架构技术白皮书[R]. 北京:中国移动,2022.
- [16] 何小强,唐伦,陈前斌. 面向6G的数字孪生网络综述:架构、应用和挑战[J]. 重庆邮电大学学报(自然科学版),2024,36(3):401-412.
- [17] Sheyner O, Haines J, Jha S, et al. Automated generation and analysis of attack graphs[C]//Proceedings of 2002 IEEE Symposium on Security and Privacy. Berkeley: IEEE,2002:273-284.

作者简介:

孙翊豪,助理工程师,硕士,主要从事网络安全管理工作;孔令飞,高级工程师,学士,主要从事网络空间安全架构设计工作;沈元,博士,主要研究方向为人工智能安全、关键信息基础设施保护等。