

移动通信网络攻防场景构建与 Cybersecurity Scenario Construction and AI Enhancement for Mobile Communication Networks AI 增强研究

孙 健^{1,2}, 葛 然³, 徐 雷^{1,2}, 郭新海^{1,2} (1. 中国联通研究院, 北京 100048; 2. 下一代互联网宽带业务应用国家工程研究中心, 北京 100048; 3. 中国联合网络通信集团有限公司, 北京 100033)

Sun Jian^{1,2}, Ge Ran³, Xu Lei^{1,2}, Guo Xinhai^{1,2} (1. China Unicom Research Institute, Beijing 100048, China; 2. Next Generation Internet Broadband Service Application National Engineering Research Center, Beijing 100048, China; 3. China United Network Communications Group Co., Ltd., Beijing 100033, China)

摘 要:

针对 5G 安全测试中场景分散、描述不统一及固定剧本变化不足的问题, 依托虚实结合的 5G 安全靶场, 构建 5GC/MEC、5G 小基站、NGAP/UDR、承载网路由器和 UPF 协议分析 5 类场景, 并采用五元框架统一描述。在此基础上, 引入大语言模型开展测试分支、参数行为、观测点和难度配置扩展。以 NGAP/UDR 场景为例, 模型生成 19 条候选, 经规则复核后保留 13 条, 并选取 C03 进行隔离验证。结果表明, 该方法能够提升场景扩展的规范性、可执行性与可观测性。

关键词:

5G 安全; 安全靶场; 场景构建; 大语言模型; UDR
doi: 10.12045/j.issn.1007-3043.2026.09.012
文章编号: 1007-3043(2026)09-0063-06
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:

To address fragmented scenarios, inconsistent descriptions, and limited variation in 5G security testing, five types of scenarios are constructed, including 5GC/MEC, 5G small cells, NGAP/UDR, transport routers, and UPF protocol analysis—on a hybrid 5G cyber range, and a five-element framework is used to describe them. Then large language models are introduced to extend test branches, parameter and behavior variations, observation points, and difficulty configurations. Taking the NGAP/UDR scenario as an example, the model generates 19 candidates, of which 13 are retained after rule-based review, and candidate C03 is further validated in an isolated environment. The results show that the proposed method can improve the standardization, executability, and observability of scenario extension.

Keywords:

5G security; Cyber range; Scenario construction; Large language model; UDR

引用格式: 孙健, 葛然, 徐雷, 等. 移动通信网络攻防场景构建与 AI 增强研究[J]. 邮电设计技术, 2026(9): 63-68.

1 概述

移动通信网络涵盖核心网、MEC、接入设备、承载网及以 UPF 为核心的用户面。各网络功能通过信令、服务化接口和数据隧道相互关联, 安全风险呈现跨节点、跨层级和多阶段特征^[1-2]。单一协议测试或固定脚本难以覆盖不同网络域的差异化风险。安全靶场可在授权、隔离环境中支持安全测试与防护验证^[9], 但现

有研究多关注平台能力、资源编排和通用场景, 面向 5G 网元及协议流程的演练场景仍缺乏统一组织, 固定剧本则存在测试路径单一、参数变化有限和观测点不足等问题。

本文构建并完成 5GC/MEC、5G 小基站、NGAP/UDR 2 个阶段组合、承载网路由器和 UPF 协议分析 5 类场景的基础验证, 采用五元场景表达框架进行统一描述, 并引入受约束大语言模型辅助生成测试分支、参数与行为变化、观测点和难度配置候选。候选由作者依据 5 项预设规则进行逐条复核, 形成直接保留、修

收稿日期: 2026-07-14

改后保留和拒绝3类结果。本文总体技术路线如图1所示。

2 移动通信网络多域攻防场景体系与构建原则

2.1 靶场基础、多域范围与构建原则

本文依托虚实结合的5G安全靶场,将物理设备、虚拟网元、协议流量和测试工具组合使用,用于还原MEC边缘节点、核心网网元、5G小基站、承载网路由器和UPF等对象。5类场景由作者团队自主设计并完成基础演练验证。本文所称“多域”包括云边缘、接入、核心网、承载和用户面等技术域,所选5类场景不代表对5G安全风险的完整分类。

场景构建遵循3个原则。首先,以实际对象和可验证步骤为基础,不为追求完整性虚构不存在的身份继承、权限传播或协议关系。其次,明确各测试阶段的前置条件和授权基础,不因活动按顺序执行而将其视为连续攻击链。最后,把可观测证据纳入场景设计,使日志、流量、协议字段、运行时事件、认证记录和配置变化能够与测试步骤对应。

2.2 统一场景表达方式

为避免不同场景仅按操作步骤罗列,本文采用“测试对象—前置与授权条件—测试阶段—观测证据—验证目标”五元框架统一描述。各要素分别说明测试涉及的资产或协议、实施所需条件、具体测试内容、用于验证过程与结果的日志和状态信息,以及预期验证事项。AI辅助扩展仅在既有资产、拓扑和授权边界内生成候选。具体如表1所示。

3 5类5G攻防场景的构建与基础验证

3.1 5GC/MEC场景

该场景组合CPE、MEC业务、容器或宿主机及核心网网元,按照“终端接入—边缘业务入口测试—容器或宿主机边界测试—核心网访问”的顺序组织演练。场景以边缘业务环境为起点,将接入过程、边缘侧测试和核心网访问纳入同一流程,形成由MEC侧向核心网侧逐步扩展的测试路径。

3.2 5G小基站场景

该场景以皮基站、网关和网管系统为对象,组合

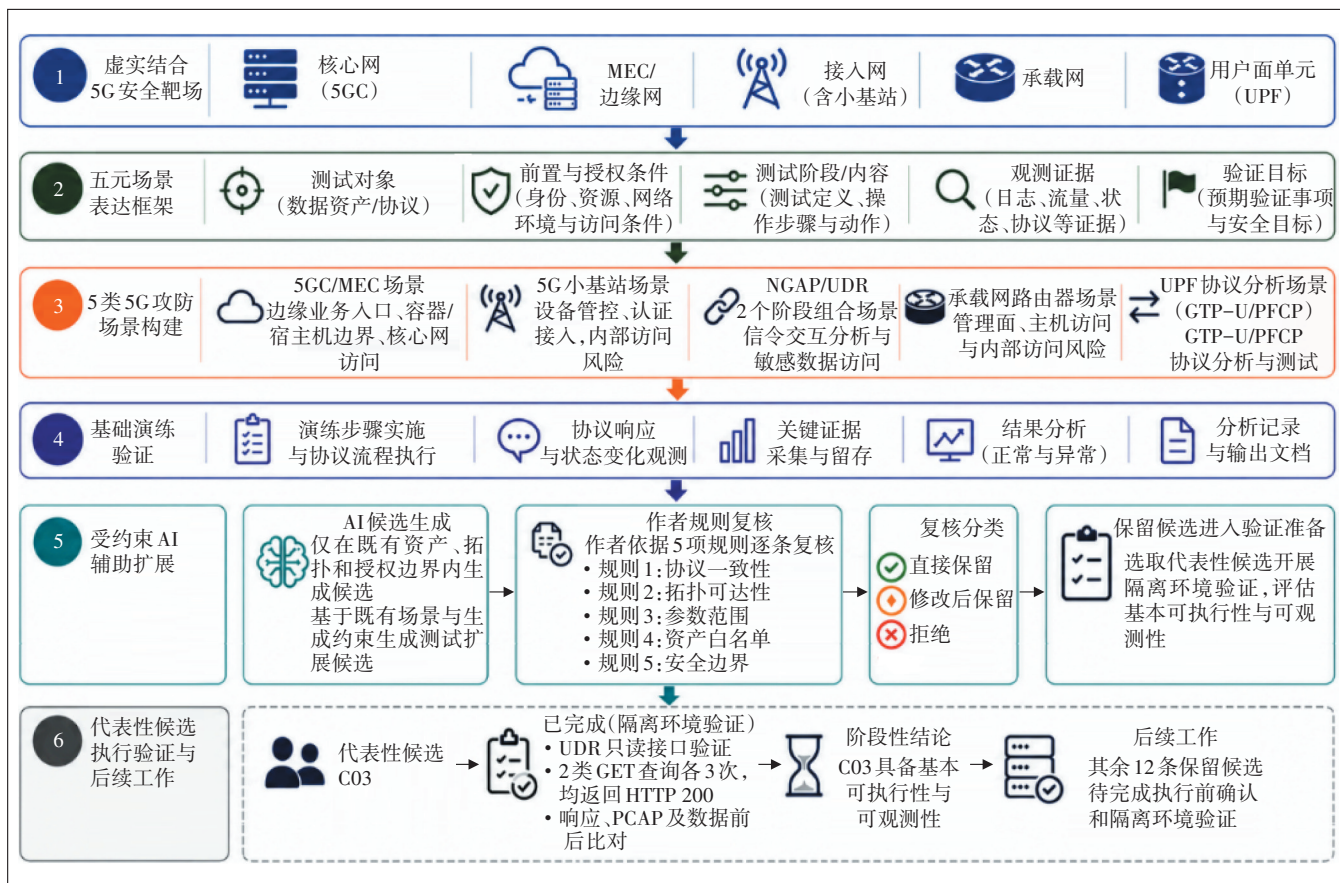


图1 5G多域攻防场景构建与AI辅助扩展技术路线

表1 5类5G多域攻防演练场景体系

场景	测试对象及前置/授权条件	基础测试阶段或演练内容	关键观测证据	验证目标
5GC/MEC	CPE、MEC业务、容器/宿主机、核心网网元、授权SIM/CPE、MEC靶场和测试核心网	网络接入,入口突破,容器/宿主机边界测试,核心网访问	Web日志、运行时事件、进程/连接、网元访问记录	边缘侧突破与核心网访问过程的可观测性
5G小基站	皮基站、网关、网管、授权设备/固件样本、测试网关和隔离接入环境	固件/身份材料检查,认证交互,异常接入,内网访问	固件哈希、身份材料、认证日志、设备指纹	设备可信、认证边界与异常接入风险
NGAP/UDR 2个阶段组合	gNB测试端、AMF、UDM、UDR,UDR阶段流量、资源标识及访问条件独立提供	NGAP协议交互,UDR数据访问分析与验证	NGAP/NAS流量、AMF事件、UDM—UDR访问记录	协议交互与敏感数据访问路径可观测性
承载网路由器	Web管理面、宿主机、路由器、授权Web服务、主机及固件/设备环境	凭证分析,主机权限扩展,内网发现,固件/接口分析	登录日志、配置变更、扫描流量、固件分析记录	管理面、内网访问与设备固件风险
UPF协议分析(GTP-U/PFCP)	UPF、GTP-U、PFCP,授权协议测试环境和本地UPF/Open5GS	GTP-U识别,PFCP接口确认,协议栈安全测试	报文头、TEID、消息类型、信息元素、会话/心跳	用户面与控制接口协议异常检测能力

授权设备、固件样本及隔离接入环境,设置固件与身份材料分析、认证交互、异常接入和内网访问等内容。在构建时先分析设备固件和身份材料,再依据获得的设备与协议特征开展认证及接入测试,形成覆盖设备可信、身份认证和接入后访问的分阶段场景。

3.3 NGAP协议分析与UDR数据访问2阶段组合场景

该场景由2个相对独立的阶段组成。第1阶段面向gNB与AMF之间的NGAP交互,设置协议流量解析和NG Setup测试;第2阶段面向UDM与UDR之间的数据访问,设置网络标识解析、资源访问分析和授权访问测试。2个阶段分别配置身份、流量、资源标识和授权条件,不将前一阶段的身份或结果直接作为后一阶段的访问权限。

3.4 承载网路由器场景

该场景组合Web管理面、宿主机和路由器设备,设置登录与凭证分析、主机权限测试、内网发现以及固件和接口分析等内容。场景按照“管理面—主机环境—路由设备”的层次组织测试,使管理入口、主机访问和设备分析形成相互衔接但边界明确的分阶段演练流程。

3.5 UPF协议分析场景(GTP-U/PFCP)

该场景以UPF为目标对象,分别围绕GTP-U用户

面协议和PFCP控制接口构建测试内容。GTP-U阶段用于识别用户面节点、TEID及消息特征,PFCP阶段用于确认控制接口,并围绕消息类型、信息元素、会话操作和心跳机制设置协议测试。2个阶段分别采用对应的协议字段和接口约束,避免将用户面探测结果直接等同于控制面访问条件^[6-7]。

3.6 5类场景的基础验证结果

5类场景均已在授权、隔离的靶场环境中完成基础演练验证,能够按照预设阶段实施,并形成协议响应、流量、日志、状态变化或分析记录等结果。具体基础验证内容、实际输出及事实依据如表2所示。

表2 5类5G攻防场景的基础验证结果

场景	基础验证内容	实际结果或输出	事实依据与状态
5GC/MEC	CPE接入,边缘业务入口测试,容器/宿主机边界测试,核心网访问	完成4阶段演练流程,形成由边缘业务入口向宿主机和核心网访问扩展的测试过程	既有测试报告与靶场实施记录,已完成基础演练验证
5G小基站	固件读取与反编译,身份材料分析,协议模拟,认证接入,内网发现	完成固件分析、身份材料提取和模拟基站接入网关等测试	固件样本、分析结果和协议交互记录,已完成基础演练验证
NGAP/UDR	NG Setup交互,NGAP/NAS流量解析,MCC/MNC提取,UDM—UDR流量分析,授权数据访问	获取NG Setup Response,完成网络标识解析和授权数据访问测试	PCAP、协议交互响应、UDM—UDR流量分析及访问结果记录,已完成基础演练验证
承载网路由器	Web凭证分析,主机权限测试,内网发现,路由器固件与接口安全分析	完成主机访问、内网发现及路由器固件与接口逻辑分析	登录、主机访问、扫描和固件分析过程记录,已完成基础演练验证
UPF协议分析	GTP-U探测,PFCP接口识别,本地UPF协议栈分析与安全测试	完成UPF节点识别、PFCP接口确认及本地协议栈安全测试	报文、端口响应、PFCP测试过程和运行状态记录,已完成基础演练验证

4 面向既有场景的AI增强方法

4.1 4类核心增强任务

AI辅助扩展建立在已完成基础验证的场景之上,不改变既有资产范围、拓扑关系和授权边界。本文将模型任务限定为测试分支扩展、参数与行为变化生成、观测点补充和难度配置4类;后续还可用于相似性比较和覆盖缺口分析。5类场景与辅助扩展任务的对应关系如表3所示。

4.2 受约束候选生成与人工审核

本文设计的受约束的大语言模型候选生成与复核流程如图2所示。模型以既有场景、网络拓扑、资产

表3 5类场景与AI增强任务映射

场景	主要 AI 增强方向	适用边界
5GC/MEC	测试分支、观测点	在边缘业务入口、容器或宿主机边界及核心网访问等既有阶段内生成候选,补充运行时和网元访问证据
5G 小基站	参数/行为变体、难度配置	围绕设备身份、认证时序和后续访问行为生成候选,确定性判断仍采用规则校验
NGAP/UDR 2 个阶段组合	测试分支、参数/行为变体、观测点、难度配置	分别在 NGAP 和 UDR 阶段内生成候选,不推荐未经验证的身份继承或跨阶段权限传递
承载网路由	管理行为变体、观测点	围绕管理登录、配置变化、扫描行为及路由或链路证据生成候选
UPF 协议分析	协议参数变化、难度配置	分别针对 GTP-U 和 PFCP 生成候选,并受字段白名单、频率及强度上限约束

关系、协议规范、历史记录和授权边界为输入,仅生成场景扩展候选,不直接执行测试操作。候选由作者依据协议一致性、拓扑可达性、参数范围、资产白名单和安全边界 5 项规则逐条复核,并分为直接保留、修改后

保留和拒绝 3 类。其中,直接保留和修改后保留仅表示通过规则复核,不代表已完成靶场验证。保留候选在满足测试授权、最小权限、数据备份、回滚和异常终止等条件的情况下,并完成执行前确认后,方可进入隔离靶场验证^[8,10]。输入资料应进行来源校验、脱敏和访问控制,候选生成、修改与处置过程均保留审计记录。

5 NGAP/UDR 场景的 AI 候选生成、作者规则复核与执行验证

本文以已完成基础验证的 NGAP/UDR 2 个阶段场景为例,使用 Claude 生成 19 条候选,由作者依据 5 项规则逐条复核,并选取 C03 开展隔离环境执行验证;其余 12 条保留候选尚待验证。

5.1 输入约束与候选生成设置

Claude 生成 19 条扩展候选,AI 仅辅助进行格式整理和重复项标记,不参与规则判定;作者依据 5 项规则

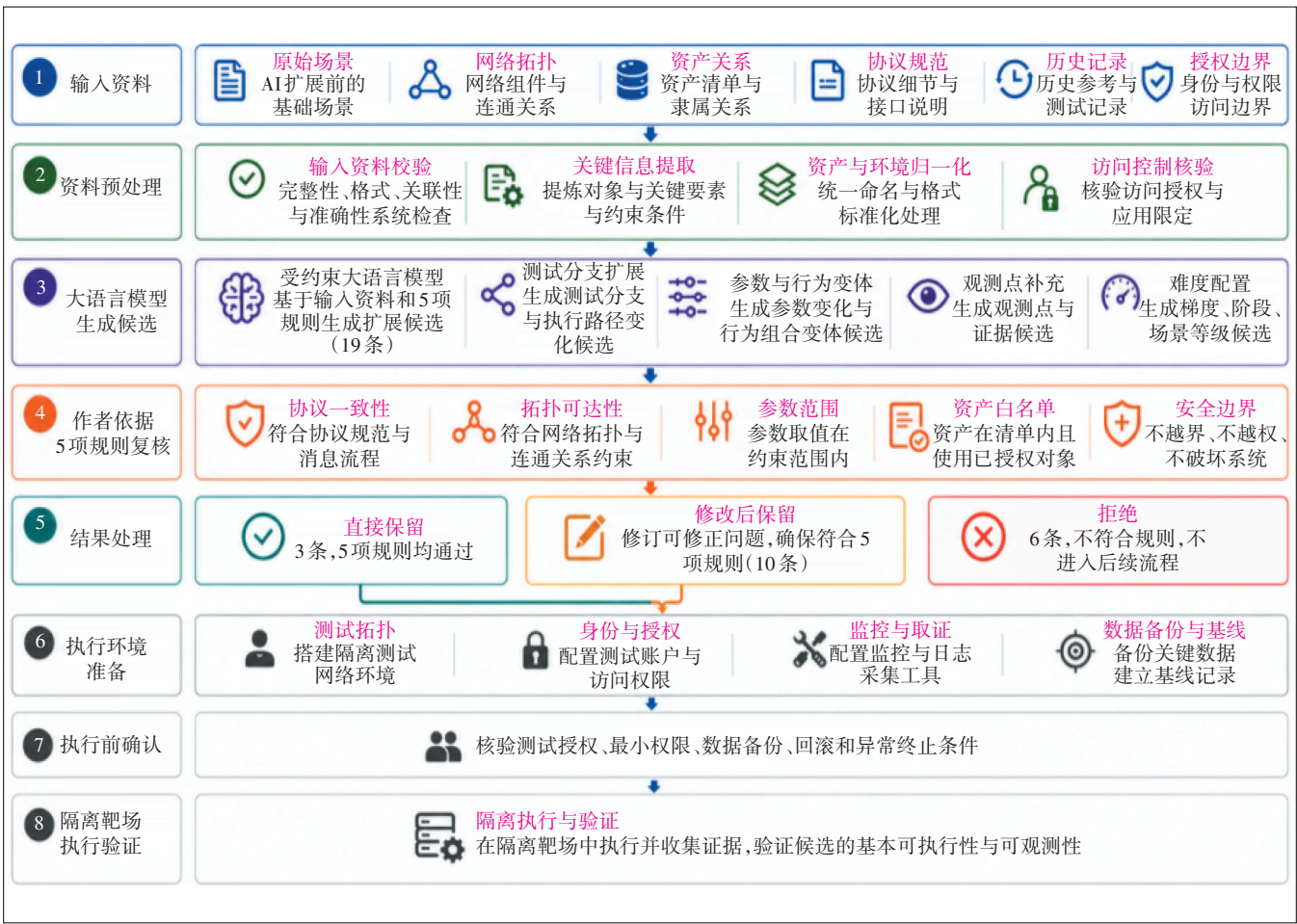


图2 受约束 AI 候选生成与复核流程

对全部候选逐条复核。NGAP/UDR 场景候选生成的提示词结构与流程如图3所示。

5.2 经规则复核后保留的代表性候选

为说明4类候选的人工复核与修订过程,每类各选取1条候选进行说明。测试分支扩展候选C01区分了请求侧 Supported TA List 与响应侧 PLMN Support List 及 Slice Support List; 参数与行为变化候选C06补充了独立 SCTP 关联或状态复位的前置条件; 观测点补充候选C11增加了 SCTP 关联、NGAP PDU 类型、NG Setup Response 或 Failure 及 Cause 等观测内容; 难度配置候选C18组合C08、C07和C14, 其中C08、C14经修订后保留,C07直接保留,且不跨越NGAP与UDR阶段的身份和权限边界。13条保留候选的复核与修订结果如图4所示。

5.3 作者规则复核结果

作者依据协议一致性、拓扑可达性、参数范围、资产白名单和安全边界5项预设规则,对19条候选逐条

人工复核,并将结果分为直接保留、修改后保留和拒绝3类,以避免将“未触发拒绝规则”直接视为有效候选。最终3条直接保留、10条修改后保留、6条拒绝(见表4)。5项规则分别检查协议流程与字段语义、既有拓扑或授权路径、参数及频率强度范围、授权资产范围,以及跨阶段权限继承、破坏性或拒绝服务风险。

10条修改后保留候选主要涉及协议语义、资源命名、信息元素属性、观测内容、只读授权范围及前置状态等可修正问题;6条拒绝候选则存在跨阶段权限继承、破坏性或拒绝服务行为、协议状态机不一致、频率强度超限及拓扑不可达等问题。

5.4 候选C03的隔离环境执行验证

完成测试授权、只读权限配置和环境确认后,选取C03开展隔离环境UDR只读接口验证。2类GET查询各重复3次,均返回HTTP 200,响应与数据库基线一致,测试端—UDR通信可观测,执行前后数据未变化。本次未验证完整UDM—UDR调用链,其余12条

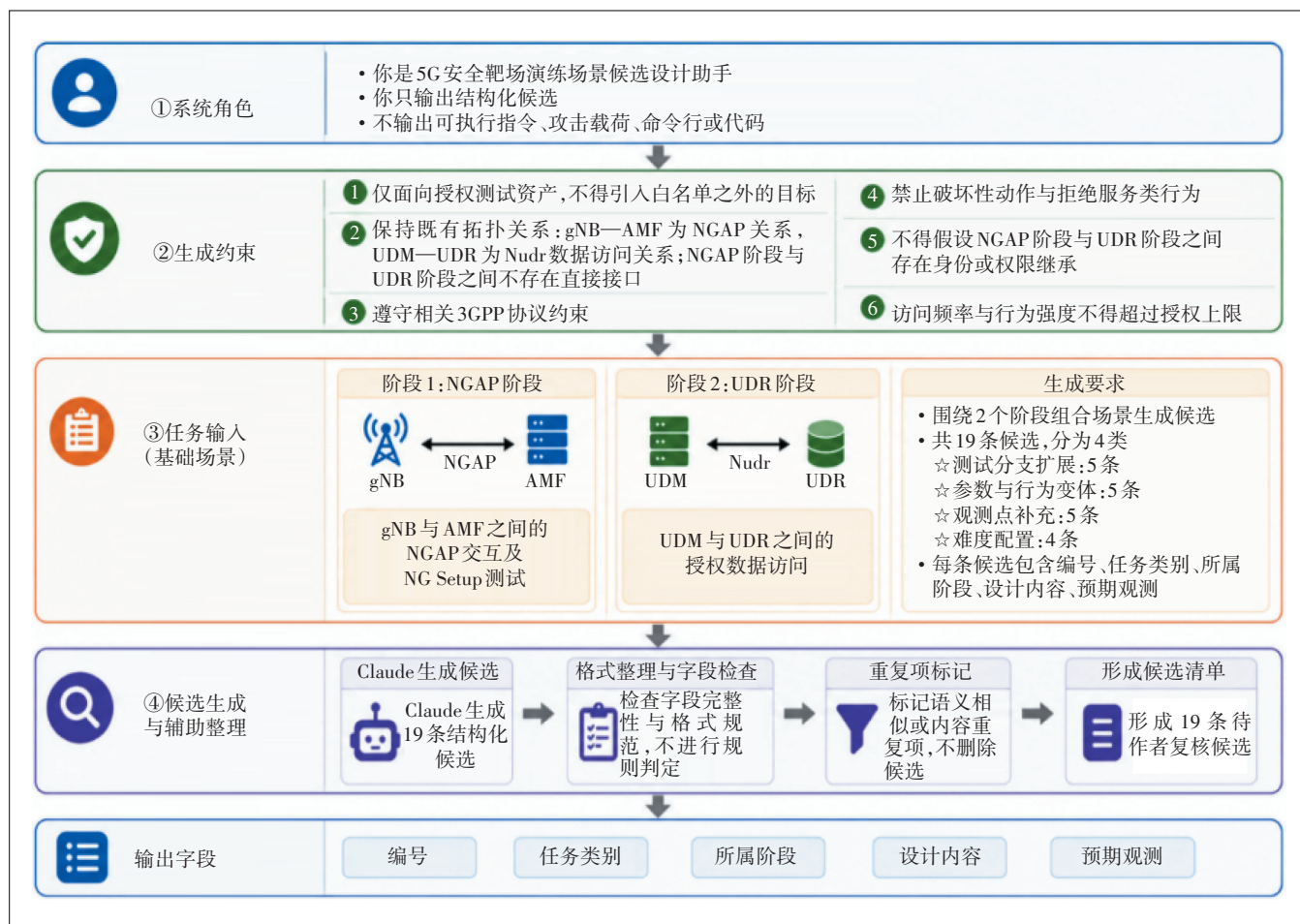


图3 NGAP/UDR 场景候选生成的提示词结构与流程

测试分支扩展 (生成更多分支与变体)			参数与行为变体 (丰富行为方式与边界)			观测点补充 (补充可观测证据)			难度配置 (形成基础/进阶/复杂级)		
候选ID	作者复核结论	修订后内容(要点)	候选ID	作者复核结论	修订后内容(要点)	候选ID	作者复核结论	修订后内容(要点)	候选ID	作者复核结论	修订后内容(要点)
C01	修改后保留	在 NG Setup Request 的 Supported TA List 中增加重复或多个 TimeSlot PLMN Item; 限制每次 AMF 响应 Setup Response 中间的 PLMN Supported List 项目 TA 列表的 record List	C06	修改后保留	补充“建立独立的 Sctp 关联”或“Sctp 关联状态复位”的前置条件,建立“新建重启并发控制”	C11	修改后保留	记录 Sctp 关联建立与心跳携带、NGAP PDU 类型、NG Setup Response 或 NG Setup Failure 结果及 Failure 或对应 Cause	C16	修改后保留(基础级)	依赖触发条件修订后形成基础级
C02	修改后保留	在请求携带的拓扑或相关 TA 列表不完整情况下,比较 NG Setup Response 或 NG Setup Failure 的差异内容与 Cause	C07	直接保留	将请求的时间窗参数等设为合法边界内,验证不同时间节奏	C12	直接保留	NAS 类型统计(仅类型/计数)	C17	修改后保留(进阶级)	依赖 C06 修订后形成进阶级,采用低频、分阶段配置
C03	修改后保留	在授权只读条件下,对 am-data 和 smf-selection-subscription-data 资源执行 GET 查询,比较响应并核验执行前后数据变化	C08	修改后保留	强化 Global RAN Node ID 组合,保留规范的 NodeID;资源选择仅对合法且存在的对象 AMF 标识维度增加组合关系覆盖	C13	直接保留	AMF 事件与审计日志观测	C18	修改后保留(复杂级)	组合 C08、C07 和 C14 形成复杂级,其中, C08、C14 经修订, C07 直接保留
						C14	修改后保留	删除 PUT/PATCH 等测试,只保留 GET 及日志;结合 GET 结果、请求 URI 路径、响应状态码、请求时间等判定访问范围			

图4 NGAP/UDR 场景 AI 候选复核与处置结果

表4 NGAP/UDR 场景 AI 增强候选的作者复核结果

增强任务类型	原始候选数	直接保留	修改后保留	拒绝
测试分支扩展	5	0	3	2
参数与行为变体	5	1	2	2
观测点补充	5	2	2	1
难度配置	4	0	3	1
合计	19	3	10	6

候选尚待验证。

6 结论

本文构建了5类5G攻防场景的基础验证,并采用五元框架进行统一描述。在NGAP/UDR案例中,Claude生成19条候选,经作者逐条进行规则复核,3条直接保留、10条修改后保留、6条拒绝。C03在隔离环境中完成2类UDR只读查询验证,6次执行均返回HTTP 200,结果与数据库基线一致且未产生数据修改。结果表明,经约束生成和人工复核的C03具备基本可执行性与可观测性,其余候选仍需进一步验证。

参考文献:

[1] 冯登国,徐静,兰晓. 5G 移动通信网络安全研究[J]. 软件学报, 2018,29(6):1813-1825.

[2] 3GPP TS 33.501 Security architecture and procedures for 5G system[S].
[3] 3GPP TS 38.413 NG-RAN;NG Application Protocol (NGAP)[S].
[4] 3GPP TS 29.504 5G System; Unified Data Repository Services; Stage 3[S].
[5] 3GPP TS 29.505 5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3[S].
[6] 3GPP TS 29.281 General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)[S].
[7] 3GPP TS 29.244 Interface between the Control Plane and the User Plane nodes[S].
[8] NIST AI 100-1 Artificial intelligence risk management framework (AI RMF 1.0)[S].
[9] Yamin M M, Katt B, Gkiotos V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture[J]. Computers & Security, 2020, 88: 101636.
[10] Lupinacci M, Blefari F, Romeo F, et al. ARCeR: an Agentic RAG for the Automated Definition of Cyber Ranges[EB/OL]. (2025-04-16) [2026-06-10]. https://arxiv.org/abs/2504.12143.

作者简介:

孙健,工程师,硕士,主要从事网络与信息安全研究工作;葛然,高级工程师,硕士,主要从事网络与信息安全研究工作;徐雷,高级工程师,博士,主要从事网络与信息安全研究工作;郭新海,工程师,硕士,主要从事网络与信息安全研究工作。