

文章编号: 2095-4980(2025)12-1239-11

基于网络靶场的重载铁路移动通信网络安全评测方法

谢克绪¹, 孙斌^{*2a,2b,2c}, 王丽鑫^{2a,2b,2c}, 冯源^{2a,2b,2c}, 刘腾^{2a,2b,2c}, 丁建文^{2a,2b,2c}

(1. 国能朔黄铁路发展有限责任公司, 河北 肃宁 062350; 2. 北京交通大学 a. 宽带移动通信铁路行业重点实验室; b. 北京市高速铁路宽带移动通信工程技术研究中心; c. 电子信息工程学院, 北京 100044)

摘要: 随着重载铁路在货物运输中承担日益重要的角色, 其宽带移动通信网络的安全性愈发关键。针对传统网络安全测试方法存在评测范围受限、资源消耗较大等局限性, 创新性地引入网络靶场技术, 用于重载铁路宽带移动通信网络安全评测。确定了数据链路层测试、接口测试、操作、管理和维护(OAM)系统安全测试、网络配置管理测试、性能压力测试、漏洞扫描与渗透测试和安全运维监控测试这7个重载铁路宽带移动通信网络安全评估指标, 阐述了每一评估指标具体测试内容。利用网络靶场模拟真实环境, 选取分布式拒绝服务攻击(DDoS)、恶意软件攻击、身份认证攻击和网络延时攻击这4个实际运营中较为常见且具有代表性的典型场景进行测试。基于4种攻防场景下得到各网元及链路在攻击下中央处理器(CPU)利用率、内存利用率、带宽、延迟、抖动和丢包率变化数据。最后使用层次分析法进行了网络风险评估, 评估结果可为重载铁路网络安全评估提供参考。

关键词: 重载铁路; 网络安全; 网络靶场; 评估指标; 层次分析法

中图分类号: TN914.42

文献标志码: A

DOI: 10.11805/TKYDA2025034

Security evaluation method for heavy-duty railway mobile communication network based on cyber range

XIE Kexu¹, SUN Bin^{*2a,2b,2c}, WANG Lixin^{2a,2b,2c}, FENG Yuan^{2a,2b,2c}, LIU Teng^{2a,2b,2c}, DING Jianwen^{2a,2b,2c}

(1. CHN Energy Shuohuang Railway Development Co., Ltd., Suning Hebei 062350, China; 2a. Key Laboratory of Railway Industry of Broadband Mobile Information Communications; 2b. Beijing Engineering Research Center of High-speed Railway Broadband Mobile Communications; 2c. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

Abstract: As heavy-haul railway plays an increasingly important role in cargo transportation, the security of their broadband mobile communication networks becomes more and more critical. Aiming at the limitations of traditional network security testing methods such as restricted evaluation scope and large resource consumption, cyber range technology is innovatively introduced to conduct the security evaluation of heavy-haul railway broadband mobile communication network. Seven security assessment indicators for the broadband mobile communication network of heavy-haul railways have been determined, including data link layer testing, interface testing, Operation, Administration, and Maintenance(OAM) system security testing, network, configuration management testing, performance pressure testing, vulnerability scanning and penetration testing, and security operation and maintenance monitoring testing. The specific testing contents of each assessment indicator are elaborated. The cyber

收稿日期: 2025-02-11; 修回日期: 2025-03-17

基金项目: 国能朔黄铁路发展有限责任公司科技资助项目(SHTL-23-32)

*通信作者: 孙斌 email:bsun@bjtu.edu.cn

引用格式: 谢克绪, 孙斌, 王丽鑫, 等. 基于网络靶场的重载铁路移动通信网络安全评测方法[J]. 太赫兹科学与电子信息学报, 2025, 23(12): 1239-1249. DOI: 10.11805/TKYDA2025034.

Citation format: XIE Kexu, SUN Bin, WANG Lixin, et al. Security evaluation method for heavy-duty railway mobile communication network based on cyber range[J]. Journal of Terahertz Science and Electronic Information Technology, 2025, 23(12): 1239-1249. DOI: 10.11805/TKYDA2025034.

range is employed to simulate the real environment, and Distributed Denial of Service(DDoS) attacks, malware attacks, authentication attacks and network delay attacks are selected as the four typical scenarios that are more common and representative in actual operation for testing. Based on the four attack and defense scenarios, the data of Central Processing Unit(CPU) utilization, memory utilization, bandwidth, latency, jitter and packet loss rate changes of each network element and link under attack are obtained. Finally, the network risk assessment is carried out using the hierarchical analysis method, and the results can be used as a reference for the security assessment of heavy-duty railroad networks.

Keywords: heavy-haul railway; cyber security; cyber range; assessment indicators; analytic hierarchy process

重载铁路^[1]作为交通基础设施的重要组成部分,承担着大量货物的运输任务,重载铁路宽带移动通信网络的安全性直接关系到铁路运输的流畅性和安全性^[2-3]。研究重载铁路宽带移动通信网络安全评估指标及测试方法能够及时发现和解决网络中的安全隐患,应对不断升级的威胁,从而保障重载铁路运输的安全。

传统的网络安全评测方法如渗透测试、漏洞扫描、安全审计^[4-7]等在实际应用中面临诸多挑战。例如,渗透测试主要依赖人工经验对已知漏洞进行局部检测,存在评测范围受限、资源消耗大、缺乏动态对抗验证等问题;漏洞扫描技术虽能快速识别系统弱点,但难以模拟复杂攻击链和未知威胁;安全审计则侧重于静态配置核查,无法全面评估网络在真实攻击场景下的动态响应能力。这些方法的局限性导致其难以适应重载铁路通信网络高实时性、高可靠性的安全需求。

智能评测技术也是一种网络安全评估的思路。基于机器学习与人工智能的自动化评测方法显著提升了测试效率和覆盖范围。此类技术能够通过历史数据训练模型,自适应生成多样化攻击场景,并实时分析网络行为中的潜在风险。然而,智能评测的落地仍面临挑战:其一,依赖高质量标注数据集,而铁路通信网络场景数据获取难度大;其二,复杂攻击行为的动态建模能力有限,难以完全替代人工经验。

在此背景下,网络靶场^[8]充分利用虚拟化、仿真和模拟等先进技术,能够高度精确地模拟重载铁路宽带移动通信网络的真实环境,进而评估网络系统的安全性。相较于传统静态测试,网络靶场可模拟多维度攻击场景,结合层次分析法量化全局风险,实现评测范围扩展与资源效率提升。同时,其支持自动化数据采集与智能算法集成^[9-11],例如利用机器学习优化攻击向量生成策略,或通过深度学习模型实时识别异常流量模式。这种“虚实结合”的评测框架既保留了传统方法的可解释性,又兼具智能技术的动态适应性,为重载铁路网络安全评估提供了有效解决方案。

本文明确了重载铁路宽带移动通信网络安全测试评估指标及各部分测试内容。此外,为了验证和完善评估指标的实施效果,首次提出通过搭建重载铁路网络安全靶场实验环境来进行网络安全测试,从整体测试方法中选取分布式拒绝服务攻击(DDoS)模拟、恶意软件攻击模拟、身份认证攻击模拟和网络延时攻击模拟这四个实际运营中较为常见且具有代表性的典型攻击场景进行实验场景设计和测试,最后基于测试数据使用层次分析法进行了网络风险评估。

1 网络安全测试评估指标

重载铁路宽带移动通信网络安全的保障离不开网络安全评估指标和测试方法的深入研究。其关键在于明确重点测试项目,形成评估指标体系^[12];探索各评估指标具体测试内容,以形成全面系统的安全测试方法,确保重载铁路通信网络的稳定运行。

网络安全测试评估项目包含数据链路层测试、接口测试、操作、管理和维护(OAM)系统安全测试、网络配置管理测试、性能压力测试、漏洞扫描与渗透测试、安全运维监控测试等。数据链路层测试、接口测试遵循铁路长期演进技术(Long-Term Evolution for Railway, LTE-R)网络分层架构特性,逐层覆盖协议栈核心安全需求,确保各层级防护无盲区;网络配置管理测试确保配置安全性与运维效率,从而支撑重载铁路通信系统的高可靠运行;OAM系统安全测试与安全运维监控测试通过审计日志、角色权限管理等手段,构建“防御-检测-响应”闭环管理体系,满足铁路行业对运维合规性的标准要求;性能压力测试与漏洞扫描聚焦于极端场景如DDoS洪泛、恶意软件渗透下的网络鲁棒性验证。7种项目的融合形成网络安全评估指标,如图1所示。

1.1 数据链路层测试

国家能源集团重载铁路宽带移动通信网络通常采用铁路长期演进技术(LTE-R),本文中提及的重载铁路宽带

移动通信网络在技术实现上主要基于 LTE-R 网络架构进行相关测试与分析。数据链路层测试主要针对 LTE-R 网络采用的安全机制进行测试验证^[13], 主要对于基站(evolved Node B, eNB)与核心网服务网关(Serving Gateway, SGW)/移动性管理实体(Mobility Management Entity, MME)之间的 S1 接口、用户设备(User Equipment, UE)与 eNB 之间的 Uu 接口、eNB 之间的 X2 等接口的数据链路层进行测试。测试内容包括以下方面:

1) 测试加密算法的强度, 从而保护用户数据的安全性。通过测试 AES-128/256 等加密算法的强度, 可以评估其抵抗各种攻击的能力, 确保用户数据在传输过程中不被窃取或篡改。

2) 测试链路层头压缩算法的有效性, 可以提高数据传输的效率。链路层头压缩算法可以减小数据包的大小, 从而节省带宽和提高传输速度, 通过测试其有效性, 可以确保在数据传输过程中头部信息能够被有效压缩, 减少网络负载和传输延迟。

3) 测试序列号封包, 从而防止重放攻击。重放攻击是指攻击者拦截并重新发送之前已经捕获的有效数据包, 以达到欺骗或破坏的目的, 通过测试序列号封包的功能, 可以验证其能够有效地识别和防止重放攻击, 保障数据传输的完整性和可靠性。

4) 测试授权机制的有效性, 确保只有授权用户能够访问链路层资源。通过测试授权机制, 可以验证其是否能够准确识别和验证用户身份, 防止未经授权的用户访问和篡改链路层资源。

针对上述需求, 可以采用黑箱测试和白箱测试两种方法。黑箱测试通过模拟真实环境下的压力和攻击, 对接口进行压力测试和渗透测试, 验证安全机制的鲁棒性和可靠性。白箱测试则需要获取设备源代码, 对加密算法进行强度分析和恶意测试, 以发现可能存在的弱点和潜在的破解风险。此外, 还需要进行性能测试, 以验证上述安全机制是否会对链路层性能产生明显的影响。



Fig.1 Safety evaluation indicators for heavy-duty railway communication network

图1 重载铁路通信网络安全评估指标

1.2 接口测试

接口测试主要针对 LTE-R 网络的接口进行测试, 包括 eNB 与核心网 SGW/MME 间的 S1 接口、UE 与 eNB 之间的 Uu 接口、eNB 之间的 X2 接口和分组数据网络网关(Packet Data Network Gateway, PGW)与外部应用系统间的 SGi 接口。测试内容包括以下几个方面:

1) 验证接口是否只允许授权主机访问, 确保只有经过授权的主机能够与接口进行通信。这样可以防止未经授权的主机进行非法访问, 保障系统的安全性。

2) 验证测试接口是否支持强密码、数字证书认证方式, 确保接口的身份认证机制的有效性和安全性。强密码和数字证书认证可以提供更高的安全级别, 防止身份伪造和信息泄露。

3) 测试接口是否采用安全传输层协议如传输层安全协议(Transport Layer Security, TLS)或互联网安全协议(Internet Protocol Security, IPsec), 确保在传输过程中数据的安全性。这些安全传输层协议可以加密传输数据, 防止数据被窃取或篡改。

4) 测试接口是否支持访问控制列表限制非法 IP 访问, 防止未经授权的 IP 地址进行非法访问和攻击。通过测试访问控制列表(Access Control List, ACL)的功能和有效性, 可以确保只有经过授权的 IP 地址能够访问接口。

5) 测试接口是否记录详细的访问日志并支持访问审计功能, 对接口的使用进行监控和审计。访问日志记录可以帮助追踪和分析接口的使用情况, 及时发现异常和安全事件。

综上所述, 可以采用如下测试方法: 通过模拟非授权主机的访问请求, 验证是否能够拒绝非法访问; 模拟各种认证方式的访问请求, 验证接口是否能够正确地进行身份认证; 模拟传输过程中的数据流, 验证是否能够正常使用安全传输层协议进行数据传输; 通过模拟非法 IP 地址的访问请求, 验证是否能够正确地拦截非法访问; 通过模拟访问请求, 验证接口是否能够正确地记录访问日志和支持审计功能。

1.3 OAM 系统安全测试

OAM 系统安全测试主要针对 LTE-R 网络管理系统进行, 测试内容包括以下几个方面:

1) 验证管理系统是否仅限授权用户访问。通过测试验证系统是否具备用户身份验证功能, 并能正确识别和限制只有授权用户才能访问管理系统的权限。

2) 验证是否采用数字证书或动态口令等强密码学方式进行认证。通过测试验证系统是否支持使用数字证书、动态口令等强密码学方式进行用户认证, 以确保认证过程的安全性和可靠性。

3) 测试是否记录完整详细的审计日志。通过测试验证系统是否能够记录必要的审计信息, 并能够提供详细的日志记录, 以便进行安全事件的追溯和分析。

4) 测试是否支持基于角色的细粒度访问控制。通过测试验证系统是否支持基于角色的访问控制, 能够对不同角色的用户进行细粒度的权限控制, 以确保系统的访问控制策略和权限管理的有效性。

5) 测试是否定期强制密码修改和账号锁定策略。通过测试验证系统是否具备定期强制用户修改密码和账号锁定策略, 以增强系统的密码安全性和防御能力。

6) 测试是否支持安全更新机制, 能及时修补系统漏洞。通过测试验证系统是否能够及时获取和应用安全更新, 以修补系统潜在的漏洞和安全隐患。

测试方法包括功能测试、压力测试和渗透测试。功能测试主要验证各项安全机制是否开启并正常工作; 压力测试在高并发情况下验证系统性能是否受影响; 渗透测试利用公开漏洞对系统进行模拟攻击, 以发现可能的安全隐患。

1.4 网络配置管理测试

网络配置管理测试主要针对 LTE-R 网络中的各种安全策略进行测试, 测试内容包括以下几个方面:

1) 测试访问控制列表(ACL)策略是否能有效限制非法主机访问核心网。核心网是重载铁路网络的重要组成部分, 包含了各核心网网元、核心路由器、服务器等关键设备和数据。测试 ACL 策略的有效性可以确保只有经过授权的主机才能访问核心网, 防止非法主机的入侵和未经授权的访问, 保护核心网的安全性、完整性和可用性。

2) 测试设备配置是否实行版本控制和审计修改。重载铁路可能包含大量的网络设备, 如路由器、交换机等。这些设备的配置信息需要进行版本控制和审计修改, 以确保配置的完整性和可追溯性。通过测试设备配置的版本控制和修改审计机制, 可以确保设备配置的安全性和可管理性, 减少配置错误和恶意修改的风险。

3) 测试是否支持安全自动化配置同步机制。重载铁路可能涉及多个地点和设备, 需要进行配置的同步和管理。测试是否支持安全自动化配置同步机制可以确保配置的一致性和正确性, 减少人为操作带来的配置错误和安全隐患。

4) 测试是否定期对配置进行安全审计, 查找安全漏洞。网络配置中可能存在一些潜在的安全漏洞, 如弱口令、未授权访问等。通过定期对配置进行安全审计, 可以发现潜在的安全漏洞, 并及时采取措施进行修复和加固, 以提升重载铁路宽带移动通信网络的安全性。

测试方法为功能测试、压力测试和渗透测试。功能测试验证各策略和机制是否开启和生效; 压力测试在高并发条件下, 测试策略是否会影响网络性能; 渗透测试利用非法手段, 比如伪装合法主机或利用已知漏洞, 试图突破策略的安全限制, 发现可能的安全问题。此外, 还可以进行模糊测试。比如对 ACL 规则输入边缘条件如空值或特殊字符, 测试系统是否有安全隐患。也可以对设备配置进行模糊测试, 输入非法格式或过长参数测试系统稳定性。

1.5 性能压力测试

性能压力测试主要通过对 LTE-R 网络进行大流量模拟攻击测试, 评估其对各种网络攻击的抗性能力, 测试内容包括以下几个方面:

1) DDoS 攻击测试: 评估铁路宽带移动通信网络对 DDoS 攻击的抗性能力。可以使用流量放大工具对试验网络入口链接进行用户数据报协议(User Datagram Protocol, UDP)和传输控制协议(Transmission Control Protocol, TCP)。协议洪泛攻击, 观察网络是否会崩溃。测试过程中需要监控网络的带宽利用率、丢包率等指标, 以评估网络的承载能力和抗攻击能力。

2) CPU 消耗性攻击测试: 评估网络设备的 CPU 消耗性攻击防护能力。可以使用加密算力攻击软件对网络设备的 CPU 进行消耗性攻击, 观察设备是否能正常工作。测试过程中需要监控设备的 CPU 使用率、内存占用率等指标, 以评估设备的性能和稳定性。

3) 入侵检测系统(Intrusion Detection System, IDS)/入侵防御系统(Intrusion Prevention System, IPS)报警功能测试: 评估网络的 IDS/IPS 报警功能是否有效。可以使用网络扫描器对网络进行端口扫描, 测试是否能触发 IDS/IPS 报警。测试过程中需要监控报警系统的响应时间和准确性, 以评估其对潜在攻击的识别和阻断能力。

4) Web 服务性能攻击测试: 评估 Web 服务的性能抗压能力。可以使用 HTTP 高并发攻击器对 Web 服务进行性能攻击, 观察是否会出现服务不可用的情况。测试过程中需要监控服务的响应时间、吞吐量等指标, 以评估其负载能力和容错性。

5) 分布式算力消耗攻击测试: 评估网络对分布式算力消耗攻击的抵御能力。可以使用加密挖矿软件对网络进行分布式算力消耗攻击。测试过程中需要监控网络的带宽利用率、设备的 CPU 使用率等指标, 以评估网络的承载能力和抗攻击能力。

测试方法采用真实攻击软件进行模拟攻击, 通过增加攻击规模、类型和并发度, 对网络进行多轮次测试。测试过程中监控网络各项指标, 包括入口带宽利用率、设备 CPU 使用率、内存占用率、链路流量等, 观察网络在不同规模攻击下的变化。同时测试网络是否能有效区分正常流量和攻击流量, 并触发相应的防御机制。

1.6 漏洞扫描与渗透测试

漏洞扫描与渗透测试^[14]是 LTE-R 网络安全测试的重要内容, 测试内容包括以下几个方面:

1) 通过使用专业漏洞扫描工具和渗透测试框架进行测试, 可以发现网络设备、服务和应用程序中的潜在漏洞和安全隐患。

2) 通过模拟攻击和利用已知漏洞的方式进行测试, 可以评估网络的安全性和防御能力。

3) 进行敏感信息泄露和代码注入等高危漏洞的测试, 可以发现系统中存在的安全隐患, 例如敏感信息的泄露风险和代码注入漏洞。

测试方法主要有两种: 黑盒测试从外部对系统进行扫描; 白盒测试需要获取部分内部信息进行更深入的测试。

1.7 安全运维监控测试

安全运维监控测试主要针对 LTE-R 网络安全监控系统本身进行测试, 测试内容包括以下几个方面:

1) 监控系统需要能够有效监测所有安全设备, 如防火墙、IDS 等。

2) 通过模拟各类攻击事件, 测试监控系统的识别和报警能力。

3) 监控系统需要能够记录详细的监控数据, 并支持回溯性查询。

4) 进行监控系统的性能测试, 可以评估在高负载情况下系统的表现, 确保系统在高并发访问下能够正常运行, 并保证监控数据的实时性和准确性。

5) 监控系统需要定期进行规则库的更新, 以获取最新的安全规则, 提升对新型威胁的检测能力。

6) 通过对监控系统进行安全性测试, 可以发现潜在的安全漏洞和配置问题。

测试方法包括功能测试、压力测试和模拟事件测试。功能测试核对监控功能; 压力测试评估性能; 模拟事件测试验证监控效果。

2 网络安全风险评估步骤

确定评估指标后, 使用层次分析法^[15]对重载铁路宽带移动通信网络进行网络安全风险评估。重载铁路宽带移动通信网络风险评估作为目标层, 评估指标作为准则层, 风险程度(低风险、中等风险、高风险)作为方案层。

具体步骤如下:

1) 构造判断矩阵 $A=(a_{ij})_{n \times n}$, 并计算判断矩阵权重向量 $W=(w_1, w_2, \dots, w_n)^T$ 。其中 n 为矩阵阶数, 即为选定的评估指标个数; a_{ij} 表示指标 i 相对于指标 j 的重要程度, 构造时采用如下标度含义: 1 表示两个指标同等重要, 3 表示指标 i 比指标 j 稍微重要, 2 为 1、3 判断的中间值。1/3 表示指标 j 比指标 i 稍微重要, 1/2 为 1、1/3 判断的中间值。 w_i 计算公式如下:

$$w_i = \frac{\bar{w}_i}{\sum_{i=1}^n \bar{w}_i} \quad (1)$$

式中 \bar{w}_i 为矩阵 A 每行的几何均值, 计算公式如下:

$$\bar{w}_i = \sqrt[n]{\prod_{j=1}^n a_{ij}} \quad (2)$$

式中 $i=1, 2, \dots, n$ 。

2) 矩阵的一致性检验。矩阵一致性指标(Consistency Index, CI, 用 I_C 表示一致性指标值)计算公式如下:

$$I_C = \frac{\lambda_{\max} - n}{n - 1} \quad (3)$$

式中: λ_{\max} 为矩阵最大特征值; n 为矩阵阶数。 λ_{\max} 的计算公式如下:

$$\lambda_{\max} = \frac{1}{n} \sum_{i=1}^n \frac{(AW)_i}{w_i} \quad (4)$$

随机一致性指标(Random Consistency Index, RI, 用 I_R 表示一致性指标值)为通过统计方法预先计算得出的经验值, 被广泛用于一致性检验。Saaty^[16]通过大量模拟计算, 得出了不同阶数 n 下对应的 RI 值表, 如表 1 所示:

表 1 不同阶数下 RI 值

Table 1 RI values at different orders of n

n	3	4	5	6	7	8	9
I_R	0.58	0.90	1.12	1.24	1.32	1.41	1.45

根据表 1 可查得矩阵阶数 n 对应的 I_R 并计算矩阵一致性比率(Consistency Ratio, CR, 用 R_C 表示一致性指标值), 其公式如下:

$$R_C = \frac{I_C}{I_R} \quad (5)$$

R_C 的值越小说明矩阵一致性越好, 一般认为当 R_C 小于 0.1 时矩阵一致性可以接受。

3) 根据平均增长率为评估指标打分, 得到风险等级。

平均增长率通过量化攻击前后关键性能参数的动态变化率, 可以综合表征网络受到攻击后的性能劣化趋势, 突破了单一指标的局限性, 能较好评估网络安全变化情况。每一评估指标的平均增长率 x_i 作为其评分依据, 其计算公式为:

$$x_i = \sum_{j=1}^k \left(\sum_{q=1}^m \frac{\tilde{y}_{ijq} - y_{ijq}}{y_{ijq}} \times 100\% \right) \times \frac{1}{k} \quad (6)$$

式中: $i=1, 2, \dots, n$; $j=1, 2, \dots, k$; $q=1, 2, \dots, m$; \tilde{y}_{ijq} 为第 i 种攻击模式下第 q 个网元或链路的第 j 个二级评估指标在受到攻击后的测量值; y_{ijq} 为第 i 种攻击模式下第 q 个网元或链路的第 j 个二级评估指标在受到攻击前的测量值, k 为每种攻击模式下的二级评估指标的个数; m 为每个二级评估指标下测量网元或链路个数。

根据平均增长率可计算得到每个评估指标对应得分 S_i , 其计算公式为:

$$S_i = 100 - \left(\frac{x_i - \min(x)}{\max(x) - \min(x)} \times (100 - 2B) + B \right) \quad (7)$$

式中 B 为偏置量。该公式将增长率线性映射到 0~100 分之间, 分数越高说明在受到攻击时其平均变化率越小, 系统越稳定。

每一评估指标得分与该指标所占总权重相乘得到最终风险评估分数 P , 其计算公式为:

$$P = \sum_{i=1}^n (S_i w_i) \quad (8)$$

表 2 为各风险状态判定标准, 根据风险评估分数 P 落入的区间可得最终风险评估结果。

表 2 各风险状态判定标准
Table 2 Criteria for determining each risk status

risk level	quantitative evaluation value	description of each risk status
low risk	$P >= 80$	the inspected system is in a high security state with low risk
medium risk	$80 > P >= 60$	the inspected system has certain security risks, but the risks are controllable and there is no probability of major dangerous accidents, which can meet the normal communication operation of the railway
high risk	$P < 60$	the inspected system has significant security risks and should be immediately reinforced for safety, and cannot operate normally

3 重载铁路网络靶场及实验场景设计

在确定了评估指标和测试方法后需对其进行测试, 网络靶场利用先进的虚拟化技术为测试提供了一个安全且与实际网络极为相似的仿真测试环境。这一环境不仅能够满足多样化的安全测试需求, 包括模拟各种网络攻击和防御策略, 还能通过自动化和智能化手段提升测试的效率与精确度。

3.1 基于网络靶场的 LTE-R 网络评估技术架构

基于网络靶场的 LTE-R 网络评估技术架构主要由基础设施层、虚拟化管理层和靶场服务层构成。

1) 基础设施层: 基础设施层作为整个架构的基础, 包含计算资源、存储资源和网络资源。计算资源为各类测试和模拟提供强大的运算能力, 确保数据处理和分析的高效性; 存储资源负责存储大量的网络配置数据、测试数据以及模拟攻击场景等信息; 网络资源则保障了网络靶场内部各组件之间以及与外部的通信连接, 构建起稳定可靠的数据传输通道。

2) 虚拟化管理层: 虚拟化管理层是实现网络靶场功能的关键部分, 通过虚拟化技术将基础设施层的物理资源转化为虚拟资源, 从而能够模拟出各种复杂的网络环境和设备。它包括虚拟网络、虚拟主机、虚拟存储和虚拟安全设备等组件。虚拟网络可以灵活配置不同的网络拓扑结构, 模拟 LTE-R 网络中的基站、核心网元等之间的连接关系; 虚拟主机能够模拟各种类型的终端设备和服务器, 如 MME、SGW 等, 以满足不同测试场景的需求; 虚拟存储为测试数据和系统配置提供存储空间, 保证数据的独立性和安全性; 虚拟安全设备如虚拟防火墙、IDS 等则用于模拟网络安全防护机制, 对模拟攻击进行检测和防御, 评估网络的安全性。

3) 靶场服务层基于虚拟化管理层提供的虚拟资源, 为用户提供了系列丰富的服务。场景管理服务允许用户根据测试需求定制各种复杂的网络攻击和防御场景, 包括 DDoS 攻击模拟、恶意软件攻击模拟等场景, 同时还能设置不同的攻击强度、目标和持续时间等参数; 资源管理服务负责对虚拟资源进行分配、调度和监控, 确保资源的合理利用和高效运行; 数据采集服务在测试过程中实时收集各网元及链路的性能数据, 如带宽、延迟等, 为后续的分析评估提供数据支持; 用户管理服务负责对访问网络靶场的用户进行身份认证、权限管理和操作记录, 确保靶场环境的安全性和用户操作的合规性。

3.2 实验场景设计

针对上文提出的各评估指标确定的具体测试方法需在网络靶场中设计实验场景来进行测试。实验场景的设计包括确定攻击方式、攻击目标、实验步骤及数据收集方法。从整体测试方法中选取 DDoS 攻击模拟、恶意软件攻击模拟、身份认证攻击模拟和网络延迟攻击模拟这 4 个实际运营中较为常见且具有代表性的典型场景来进行场景设计和测试。表 3 为设计的实验场景的具体实验步骤和攻击方式。

4 网络拓扑及实验结果

4.1 网络拓扑图

依照重载铁路宽带移动通信网络 LTE-R 网络架构, 搭建图 2 所示网络拓扑, 其中网元分别为 eNB、MME、SGW、PGW、归属用户服务器(Home Subscriber Server, HSS)、策略和计费规则功能(Policy and Charging Rules Function, PCRF)和 UE。PGW 向外连接各应用系统, 如无线重联系统、调度通信系统、可控列尾系统。基于以

上网络拓扑图进行上述实验场景的测试。

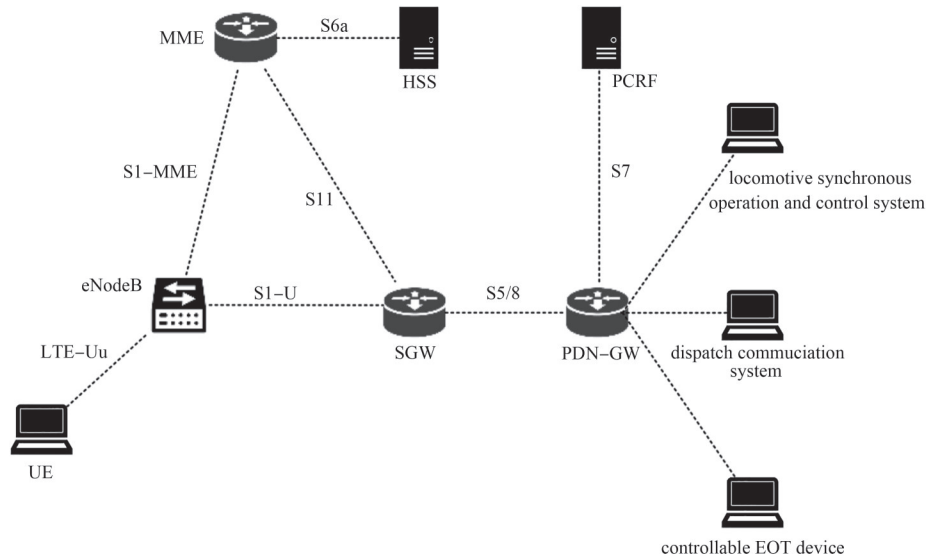


Fig.2 LTE-R network topology
图2 LTE-R网络拓扑图

表3 靶场实验场景设计场景

Table3 Design scenarios of experimental scene for shooting range

scene	DDoS attack simulation	malicious software attack simulation	identity authentication attack simulation	network latency attack simulation
attack mode	Distributed Denial of Service(DDoS) attack	malicious software propagation attack	password cracking and identity forgery attacks	network latency attack
attack target	the core router and critical links of a simulated heavy-duty railway broadband mobile communication network	simulated heavy-duty railway broadband mobile communication network business application server and critical links	identity authentication system and critical links of simulated heavy-duty railway broadband mobile communication network	key links of simulated heavy-duty railway broadband mobile communication network
experiment step	1.simulate multiple malicious hosts initiating a large number of requests to the core router, causing network congestion. 2.monitor the changes in bandwidth, latency, CPU utilization, and other related indicators before and after, and observe the impact of DDoS attacks on communication quality.	1.inject malicious software into the business application server and simulate the process of malware propagation. 2.monitor performance changes such as server bandwidth, latency, and packet loss rate, and observe the impact of malicious software propagation on communication quality.	1.attempt to use brute force password cracking to attack the identity authentication system. 2.falsifying identity information in an attempt to bypass the identity authentication system. 3.monitor performance indicators such as packet loss rate and latency of the identity authentication system, and observe the impact of identity authentication attacks on communication quality.	1.add artificial delay in critical links and simulate delay attacks. 2.monitor link latency, bandwidth, and other performance indicators to observe the impact of latency on communication quality.
data collection methods	record the changes in six key performance indicators, including CPU utilization, memory utilization, bandwidth, latency, jitter, and packet loss rate, before and after the attack			

4.2 受攻击网元设置及测试结果

在网络环境中，多样化的攻击场景各自精准地作用于特定的网元和链路，表4为不同攻击场景下受攻击网元和链路设置。对于4种攻击类型，分别测试了其单个网元和链路的影响。在对单个网元进行攻击时，通过观察各网元攻击前后CPU使用率和内存使用率来进行评估。对链路进行评估时，通过攻击该链路中其中一个网元，来观察链路的带宽、延迟、抖动和丢包率来评估其影响。为了方便描述各链路，将8条链路标记为 $L_1 \sim L_8$ 。

图3为各网元在4种攻击场景下CPU和内存使用率前后变化。对于大多数网元，受到攻击后CPU使用率和内存使用率都有所增加。DDoS攻击和恶意攻击对CPU使用率和内存使用率的影响较为显著，尤其是在PGW、SGW和eNB等网元上，以DDoS攻击为例，SGW的CPU使用率和内存使用率在受到攻击后增长幅度可达40%和

10%。身份认证攻击和延时攻击对 CPU 使用率和内存使用率的影响相对较小, 大部分网元在受到攻击后增长幅度不超过 10%。

表 4 不同攻击场景下受攻击网元设置
Table4 Settings of attacked network elements in different attack scenarios

attack category	attacking network element objects	attack link
DDoS attack	PGW,SGW,PCRF	PGW-SGW(L_3),SGW-eNB(L_7),PCRF-PGW(L_2)
malicious software attack	eNB,PGW,SGW	UE-eNB(L_6),eNB-SGW(L_7),PGW-SGW(L_3)
identity authentication attack	HSS,PCRF,MME	UE-eNB(L_6),eNB-MME(L_1),MME-HSS(L_8)
delay attack	SGW,PGW,eNB	SGW-PGW(L_3),PGW Application System(L_4),eNB SGW(L_7)

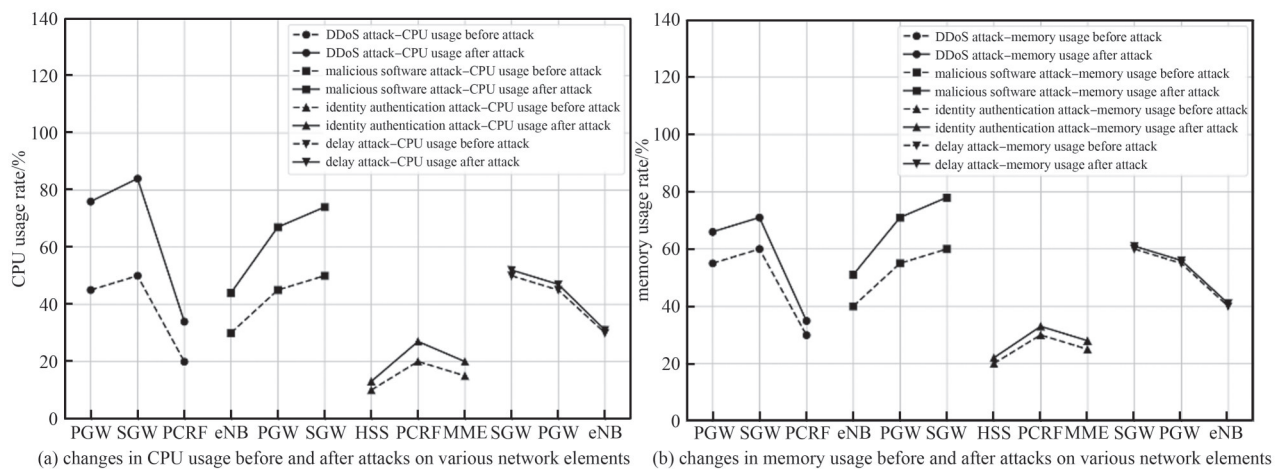


Fig.3 Changes in CPU and memory usage of each network element before and after different attack scenarios

图 3 各网元在不同攻击场景下 CPU 和内存使用率前后变化

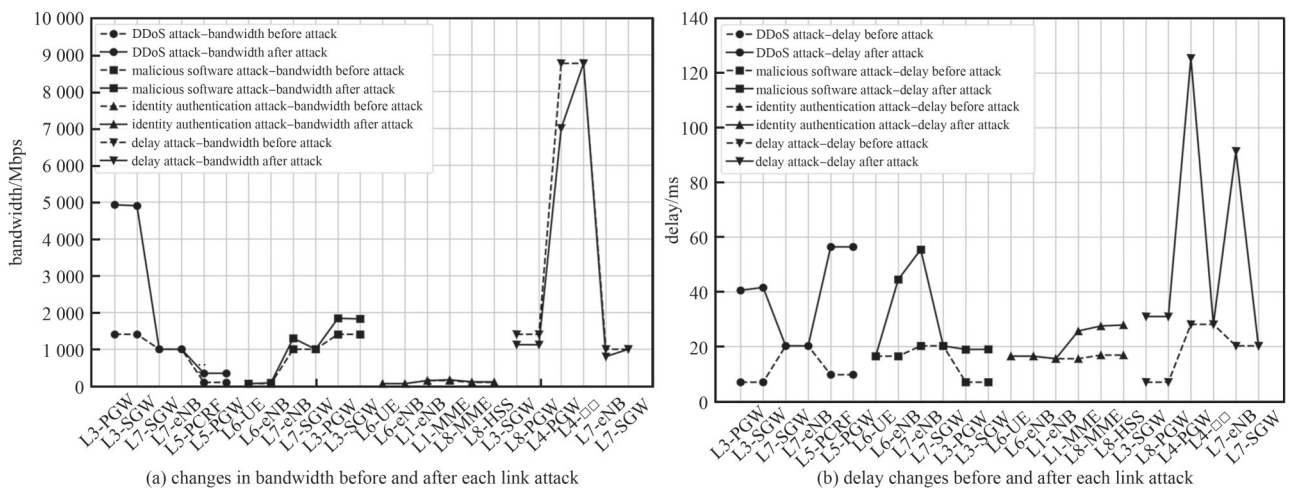


Fig.4 Changes in bandwidth and delay of each link before and after different attack scenarios

图 4 各链路在不同攻击场景下带宽和延迟前后变化

图 4 和图 5 为各链路在 4 种攻击场景下带宽、延迟、抖动和丢包率前后变化, 横坐标 L_3 -PGW 表示对于 L_3 链路上的 PGW 网元施加攻击后对链路的影响。从整体来看, 多数链路在遭受攻击后, 其带宽、延迟、抖动和丢包率呈现上升趋势。在带宽方面, DDoS 攻击的影响较为显著, 以 L_3 链路为例, 当 PGW 和 SGW 受到 DDoS 攻击后, 链路带宽会增长至攻击前的 3 倍, 而在其他类型的攻击下, 带宽变化相对较小。关于延迟, 延迟攻击对其影响最为突出, 当 L_4 链路中的 PGW 受到延迟攻击后, 延迟会增加 100 ms。在抖动指标上, DDoS 攻击、恶意攻击和延迟攻击都对其产生较大影响, L_4 链路中的各应用系统在受到上述攻击后, 抖动大约会增加 14 ms。对于丢包率的变化, DDoS 攻击和恶意攻击的影响较大。以 L_3 链路网元为例, 在受到这两种攻击后, 丢包率会增加至未受攻击时的 4 倍左右。

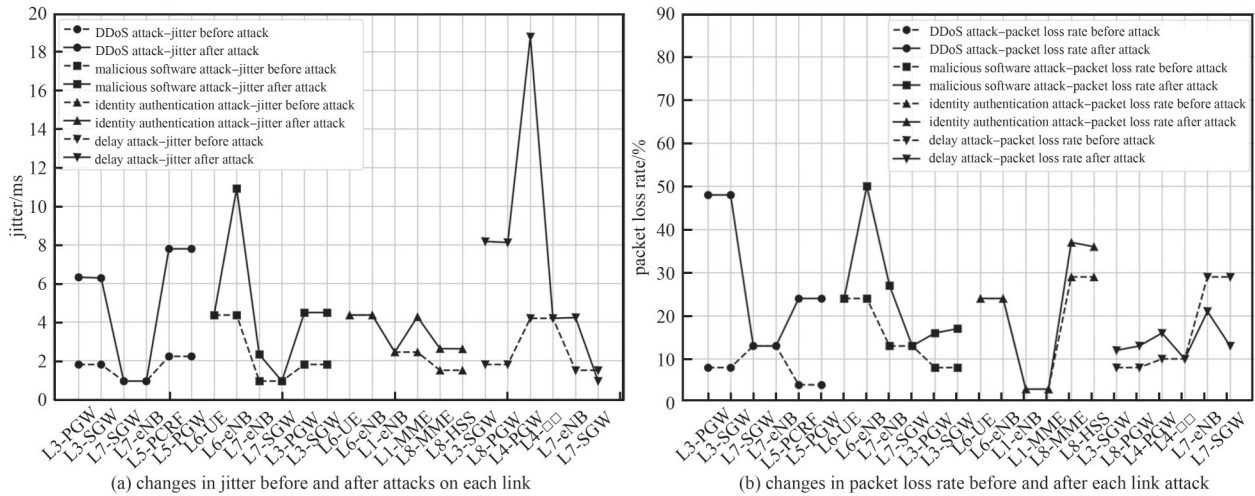


Fig.5 Changes in jitter and packet loss rate of each link before and after different attack scenarios
图 5 各链路在不同攻击场景下抖动和丢包率前后变化

4.3 风险评估计算过程

确定评估指标、得到测试数据后，使用第 2 章提到的层次分析法对重载铁路宽带移动通信网络进行网络安全风险评估。重载铁路宽带移动通信网络风险评估作为目标层，将进行测试的 DDoS 攻击、恶意软件攻击、身份认证攻击、延时攻击作为准则层，风险程度(低风险、中等风险、高风险)作为方案层。判断矩阵 A 构造为 A=

$$\begin{bmatrix}
 1 & 1/2 & 1/3 & 1/3 \\
 2 & 1 & 1 & 1 \\
 3 & 1 & 1 & 1 \\
 3 & 1 & 1 & 1
 \end{bmatrix}$$

，权重计算结果为： $W = [0.11 \ 0.29 \ 0.32 \ 0.32]$ ，由式(5)计算可得判断矩阵的 R_C 值为 0.013，

小于 0.1，通过了一致性检验，确保了矩阵构建的合理性。

由式(6)计算可得平均增长率 $x = [146\% \ 57\% \ 22\% \ 56\%]$ 。公式中 k 为每种攻击模式下的二级评估指标，本文中为 CPU 利用率、内存利用率、带宽、延迟、抖动和丢包率，故 k 的值为 6。 m 为每种攻击模式下测量网元或链路个数，当测量单个网元时 m 的值为 3，当测量链路时 m 的值为 6。在设置 offset 的值为 20 的条件下，由式(7)计算可得 $S = [20 \ 63 \ 80 \ 64]$ 。由式(8)计算可得评估分数 P 为 66.55，最终根据表 3 风险状态判定表可得出系统处于中等风险。

根据上述结果可以为重载铁路网络安全性评估提供参考，为后续优化监控策略和升级提供依据，保障网络安全工作的有效开展。

5 结论

本文提出数据链路层测试、接口测试、OAM 系统安全测试、网络配置管理测试、性能压力测试、漏洞扫描与渗透测试和安全运维监控测试这 7 项重载铁路宽带移动通信网络安全评估指标，以及每一项评估指标具体测试内容。此外，考虑到传统网络安全测试方法在评测范围、资源消耗方面存在局限性，使用网络靶场技术来进行网络安全测试。选取 DDoS 攻击、恶意软件攻击、身份认证攻击和网络延时攻击这 4 个实际运营中较为常见且具有代表性的典型场景来进行测试，4 种攻击场景分别对单独网元及关键链路进行测试，CPU 利用率、内存利用率、带宽、延迟、抖动和丢包率这 6 个二级评估指标用来评估攻击影响。最后使用层次分析法进行网络风险评估，评估结果可为重载铁路网络安全性评估提供参考。该研究思路和方法将来可借鉴到我国铁路下一代移动通信系统 5G-R 网络安全的相关工作研究中。未来研究可从以下方向深化：a) 细化网络靶场测试技术，构建标准化攻击场景库与自动化数据采集机制，提升评测覆盖度与可复现性；b) 探索智能评测技术的集成，如基于强化学习的自适应攻击向量生成、机器学习驱动异常流量实时检测等，逐步降低对人工经验的依赖；c) 结合新兴技术增强防护体系，例如引用区块链^[17]等新兴技术增强网络安全防护，确保重载铁路网络安全始终适应行业发展需求。

参考文献:

- [1] 钟章队,艾渤,陆平,等.综合轨道交通 5G 应用技术白皮书[R].北京:北京交通大学,2019.(ZHONG Zhangdui,AI Bo,LU Ping, et al. White paper on 5G application technology for integrated rail transit[R]. Beijing:Beijing Jiaotong University, 2019.)
- [2] 刘国梁,姚洪磊,解辰辉,等.基于层次分析法的铁路网络安全检查评价方法研究[J].铁路计算机应用,2023,32(11):6-10.(LIU Guoliang,YAO Honglei,XIE Chenhui,et al. Evaluation method of railway network security inspection based on analytic hierarchy process[J]. Railway Computer Application, 2023,32(11):6-10.) DOI:10.3969/j.issn.1005-8451.2023.11.02.
- [3] 梁雅楠,刘昌瑞,石雪涛.面向列车自主运行的边缘智能系统[J].太赫兹科学与电子信息学报,2024,22(8):893-900.(LIANG Yanan,LIU Changrui,SHI Xuetao. Edge intelligent system for autonomous train operation[J]. Journal of Terahertz Science and Electronic Information Technology, 2024,22(8):893-900.) DOI:10.11805/TKYDA2023071.
- [4] 邓立红.我国重载铁路运输通道发展研究[J].中国铁路,2020(8):70-75.(DENG Lihong. Development research on transportation corridors of heavy-haul railways in China[J].China Railway, 2020(8):70-75.) DOI:10.19549/j.issn.1001-683x.2020.08.070.
- [5] 张彦,司群,冯凤娟.铁路网络安全测评体系研究[J].信息安全研究,2020,6(8):738-743.(ZHANG Yan,SI Qun,FENG Fengjuan. Research on railway cyber security testing and evaluation system[J]. Information Security Research, 2020,6(8):738-743.)
- [6] 冯凯亮,张德栋,陈勋,等.铁路网络安全等级保护管理系统研究[J].铁路计算机应用,2020,29(8):66-70.(FENG Kailiang,ZHANG Dedong,CHEN Xun, et al. Railway network security level protection management system[J]. Railway Computer Application, 2020,29(8):66-70.) DOI:10.3969/j.issn.1005-8451.2020.08.016.
- [7] 祝咏升,姚洪磊,崔伟健.铁路网络安全靶场设计与研究[J].铁路计算机应用,2021,30(8):52-56.(ZHU Yongsheng,YAO Honglei,CUI Weijian. Design and research on railway network shooting range[J]. Railway Computer Application, 2021,30(8):52-56.) DOI:10.3969/j.issn.1005-8451.2021.08.11.
- [8] 李雨,李江丰.关于网络安全渗透测试流程及方法的研究[J].通信管理与技术,2024(1):42-44.(LI Yu,LI Jiangfeng.Research on the process and method of network security penetration testing[J]. Communications Management and Technology, 2024(1):42-44.) DOI:10.3969/j.issn.1672-6200.2024.01.024.
- [9] 王鑫.网络安全测评中 Web 应用安全渗透测试方法分析[J].无线互联科技,2023,20(4):165-168.(WANG Xin. Analysis of web application security penetration testing methods in network security evaluation[J]. Wireless Internet Technology, 2023,20(4):165-168.) DOI:10.3969/j.issn.1672-6944.2023.04.048.
- [10] 熊文祥,陈永刚.基于集对可拓和改进层次分析法的铁路通信系统安全评估[J].计算机系统应用,2022,31(2):285-290.(XIONG Wenxiang,CHEN Yonggang. Safety evaluation of railway communication system based on set pair extension and improved analytic hierarchy process[J]. Computer Systems & Applications, 2022,31(2):285-290.) DOI:10.15888/j.cnki.csa.008314.
- [11] 司群,田文,陈彤.建立铁路三位一体网络安全测评指标库研究[J].铁路计算机应用,2020,29(8):38-42,47.(SI Qun,TIAN Wen,CHEN Tong. Establishment of railway trinity network security evaluation index database[J]. Safety Detection and Evaluation, 2020,29(8):38-42,47.) DOI:10.3969/j.issn.1005-8451.2020.08.010.
- [12] 刘国梁,姚洪磊,解辰辉,等.基于层次分析法的铁路网络安全检查评价方法研究[J].铁路计算机应用,2023,32(11):6-10.(LIU Guoliang,YAO Honglei,XIE Chenhui,et al. Evaluation method of railway network security inspection based on analytic hierarchy process[J]. Safety Detection and Evaluation, 2023,32(11):6-10.) DOI:10.3969/j.issn.1005-8451.2023.11.02.
- [13] 陈世康,郭爽,唐晋,等.多信道数据碎片化传输安全性证明[J].太赫兹科学与电子信息学报,2023,21(3):371-377.(CHEN Shikang,GUO Shuang,TANG Jin,et al. Multi-channel data fragmentation transmission security proofs[J]. Journal of Terahertz Science and Electronic Information Technology, 2023,21(3):371-377.) DOI:10.11805/TKYDA2021179.
- [14] 王海涛,宋丽华,张国敏.网络靶场研究现状与关键技术分析[J].保密科学技术,2020(9):46-51.(WANG Haitao,SONG Lihua,ZHANG Guomin.Current status and key technology analysis of network shooting range research[J]. Confidentiality Science and Technology, 2020(9):46-51.)
- [15] 蓝炫勉,陈刚,李周,等.基于虚拟化技术的智能制造网络安全靶场设计[J].自动化博览,2023,40(7):34-37.(LAN Xuanmian,CHEN Gang,LI Zhou,et al. Design of intelligent manufacturing cybersecurity testbed based on virtualization technology[J]. Automation Panorama, 2023,40(7):34-37.) DOI:10.3969/j.issn.1003-0492.2023.07.022.
- [16] SAATY T L. The analytic hierarchy process[M]. New York:McGraw-Hill, 1980.