3 风机直流改造路线的综合评价与优选方法

3.1 综合评价指标体系的构建

3.1.1 技术性维度

后端支持能力：评估方案能否满足绿电制氢的后端要求。能量捕获与效率：评估改造后风机在全风速范围内的运行效率，以及整个风电场集电系统的损耗降低程度。电能质量：评估电流的谐波畸变率、闪变等指标。控制系统复杂性与成熟度：评估控制策略的设计难度、系统稳定性以及该技术路线的工程应用成熟度。

3.1.2 经济性维度

初始投资成本：包括设备采购成本、安装施工成本、设计咨询费用等。运营与维护成本：改造后系统的预计故障率、维护周期、备品备件费用及人员技术要求。全生命周期成本：综合考虑初始投资和未来多年的运营维护成本，折现至当前的价值。投资回报率与投资回收期：基于发电量提升、运维费用节约、可能获得的电网辅助服务收益等，计算经济回报。

3.1.3 可靠性维度

系统可用率：预计改造后风机的年可发电时间。关键设备寿命与可靠性：核心电力电子器件 . 电容等的预计寿命和失效率。故障影响范围与可维护性：单一部件故障是仅影响单机，还是影响一个汇集回路？故障诊断和修复的便捷性如何？对原有设备的依赖性：方案对原有发电机、齿轮箱等设备状态的依赖程度，是否会加剧其磨损。

3.2 优选决策流程与方法

3.2.1 信息采集与约束筛选阶段

明确改造目标：首要任务是厘清改造的核心驱动力。是为了满足强制的并网新规？是为了提升发电量？还是为了解决绿电消纳？目标不同，决策的侧重点截然不同。全面评估现状：对风电场进行彻底“体检”，包括：机组类型、运行年限、健康状况、风资源状况、现有集电线路与升压站容量、电网接入点的技术要求等。

3.2.2 定性分析与定量评价相结合的综合评价阶段

建立层次结构模型，将总目标分解为技术性、经济性、可靠性、适配性等准则层，并进一步细化为具体指标层。采用专家打分和层次分析法确定各层级指标的权重，例如，若电网薄弱，则“并网支持能力”的权重应提高。对通过初筛的方案进行评分，经济性指标定量计算，技术性、可靠性等指标则定性量化。最后，根据各指标的得分和权重计算方案的综合得分，以评估其优劣。

3.2.3 敏感性分析与最终决策阶段

进行敏感性分析：考察关键参数波动时，各方案综合得分的稳定性。找出影响决策结果的最敏感因素。

风险识别与预案：对得分最高的方案，进行全面的风险识别。特别是对于技术较新或可靠性数据不足的方案，必须评估其潜在风险并制定应对预案。

4 结语

风机直流改造是风电存量资产激活与风电场更新的关键技术，有全功率变流器、直流并联汇集、混合型三种改造路线，选适配路径很重要。

未来，电力电子等技术成熟、绿电制氢发展、风机工艺进步，将推动该技术升级；人工智能与大数据的应用，也能优化改造方案与方法。

参考文献

[1] 贾利渊,李婷婷,包晶晶,等.《商用空调风机用直流无刷电动机技术规范》团体标准解读 [J]. 中国标准化, 2025, (15): 184-189.

[2] 马骞,朱益华,谢惠藩,等. 抑制风火打捆交直流外送系统暂态过电压的风机关键控制参数优化方法 [J]. 可再生能源, 2025, 43 (07): 970-978.

[3] 魏博,吴斌,呼鹏伟,等. 大规模新能源直流外送系统下的风机高电压穿越控制参数优化方法 [J]. 能源与环保, 2025, 47 (04): 238-247.

 DOI: https://doi.org/10.12349/tie.v2i6.7804

Research on computer network security protection technology based on machine learning

Zhen chao Ma

Wuhan First Commercial School, Wuhan, Hubei, 430000, China

Abstract

To address the limitations of traditional cybersecurity protection technologies in handling unknown and dynamic threats, this paper investigates machine learning-based defense techniques. It analyzes their applications across four key scenarios: Intrusion Detection and Prevention (including data processing, multi-paradigm detection, and dynamic response), Malicious Code Detection (static/dynamic feature extraction and anti-antivirus design), Traffic Anomaly Analysis (multi-dimensional features and anomaly attribution), and Identity Authentication and Access Control. The study constructs a hierarchical collaborative defense framework, clarifying objectives, functional hierarchies, and critical technologies such as data fusion and model updates. It examines challenges like data quality and attack resistance while outlining future research directions, providing insights for enhancing intelligent defense capabilities.

Keywords

machine learning; network security protection; intrusion detection; malicious code detection

基于机器学习的计算机网络安全防护技术研究

马振超

武汉市第一商业学校，中国·湖北 武汉 430000

摘　要

为解决传统网络安全防护技术应对未知、动态威胁的局限，本文研究基于机器学习的防护技术：分析其在入侵检测与防御（含数据处理、多范式检测与动态响应）、恶意代码检测（静态/动态特征提取及抗“免杀”设计）、流量异常分析（多维度特征与异常归因）、身份认证与访问控制四大场景的应用；构建分层协同的防护系统框架，明确目标、层级功能及数据融合、模型更新等关键技术；剖析数据质量、对抗攻击等挑战并展望未来方向，为提升防护智能化提供参考。

关键词

机器学习；网络安全防护；入侵检测；恶意代码检测

1 引言

随着网络普及，恶意攻击、数据泄露等威胁常态化，传统依赖特征码、静态规则的防护技术因检测滞后、难以应对未知攻击显局限。机器学习凭借数据驱动、自适应学习优势为防护升级提供新路径，本文围绕其在四大核心防护场景的应用、防护系统框架设计、技术挑战与展望展开研究，旨在丰富理论体系，提升网络安全防护智能化水平，应对新型威胁。

【作者简介】马振超（1982–），男，回族，中国湖北武汉人，本科，讲师，从事计算机研究。

2 机器学习在网络安全防护中的核心应用技术分析

2.1 基于机器学习的入侵检测与防御技术

在基于机器学习的入侵检测与防御技术中，数据处理是保障检测精度的基础前提，需通过多维度操作实现数据价值挖掘：网络流量特征提取需从传输层、应用层协议中捕捉端口使用频率、数据包大小分布、会话持续时间等关键信息，同时从系统日志、应用日志中筛选与访问行为、指令执行相关的有效数据；日志数据清洗与归一化则针对冗余日志、格式混乱数据进行过滤与标准化，消除符号差异、数值量级偏差对模型训练的干扰；冗余特征降维则借助主成分分析、线性判别分析等方法，剔除特征间的相关性冗余，降低模型计算复杂度。在此基础上，不同机器学习范式形成互补的入侵检测逻辑：监督学习依托已标注的攻击样本，通过支持向量机、随机森林等算法构建分类模型，实现对已知入侵类型的

精准识别；无监督学习无需样本标注，通过 K-means、孤立森林等算法挖掘数据内在分布规律，定位偏离正常行为模式的未知入侵；半监督学习则结合少量标注样本与大量未标注样本，在标签稀缺场景下提升检测模型的泛化能力。而入侵防御的动态响应机制，需以检测结果为依据，通过机器学习模型对攻击趋势进行预测，自动调整防火墙规则、入侵防御系统策略，并生成威胁阻断决策，实现从“被动检测”到“主动防御”的转变[1]，如图 1 所示。

图 1 入侵防御系统动态响应流程图

2.2 基于机器学习的恶意代码检测技术

恶意代码的特征提取需兼顾静态与动态维度：静态特征提取聚焦 PE 文件的结构信息，无需运行代码即可完成初步特征捕捉；动态特征提取则需在沙箱环境中执行代码，记录进程创建、线程操作、注册表修改、系统调用序列等行为数据，反映恶意代码的实际破坏意图。针对这些特征，机器学习形成差异化的检测应用路径：分类模型如逻辑回归、卷积神经网络，通过学习正常程序与恶意代码的特征差异，实现二者的高效区分；聚类模型如 DBSCAN、层次聚类，则通过挖掘恶意代码变种间的特征相似性，完成对未知恶意代码变种的归类识别。面对恶意代码的“免杀”技术，机器学习需通过特征鲁棒性设计，筛选不易被篡改的核心特征，并强化动态行为建模，避免仅依赖静态特征导致的检测失效，提升对变异恶意代码的识别能力[2]。

2.3 基于机器学习的网络流量异常分析技术

网络流量的特征工程需覆盖多维度关键信息：时序特征反映流量在时间维度的变化规律，如单位时间内的数据包数量、流量峰值出现时刻；统计特征包括数据包大小均值、方差、协议分布占比等量化指标；协议特征聚焦 TCP、UDP、HTTP 等协议的字段异常，如异常的标志位组合、非标准端口的协议传输；流量分布特征则关注流量在不同 IP、端口间的分布均衡性。正常流量模型的构建，需依托历史正常流量数据，通过机器学习算法学习正常流量的分布模式，并建立动态更新机制，结合新增的正常流量数据迭代优化模型，适应网络拓扑、业务需求变化带来的流量模式调整。在异常检测与归因阶段，模型通过对比实时流量与正常模型的偏差程度，结合自适应调整的异常阈值判断异常流量；同时，基于流量特征与历史异常案例的关联分析，初步判断异常类型，为后续处理提供方向。

2.4 基于机器学习的身份认证与访问控制技术

行为生物特征的机器学习建模，需捕捉用户操作过程中的独特模式：键盘输入节奏包括按键间隔时间、按键持续时长、错误按键修正频率等，鼠标移动轨迹涵盖移动速度、加速度、点击间隔等特征，终端操作习惯则包括文件访问路径、应用启动顺序、操作频率等；通过机器学习算法对这些特征进行建模，形成用户独有的行为基线。基于该基线，异常登录检测可实时对比当前登录用户的行为数据与基线的偏差：若用户登录设备、地理位置无异常，但行为模式显著偏离基线，模型则判定为异常登录行为并触发告警。在动态访问控制层面，机器学习需根据用户的实时行为数据计算风险评分，如频繁访问敏感文件、在非工作时段进行高权限操作会提升风险评分，系统则依据风险评分动态调整用户权限，如降低高风险用户的操作权限、限制敏感资源访问，实现权限与用户行为风险的动态匹配，如图 2 所示。

图 2 动态访问控制中机器学习风险评分机制

3 基于机器学习的网络安全防护系统设计框架

3.1 系统设计目标

基于机器学习的网络安全防护系统设计需先明确核心目标与关键性能指标，为系统构建提供方向指引。核心目标层面，实时威胁检测旨在缩短攻击发现周期，应对网络攻击“瞬时性”特点，避免攻击扩散造成更大损失；精准攻击识别聚焦降低对正常网络行为的误判，通过机器学习模型对攻击特征的深度学习，减少因误识别导致的业务中断；自适应防护响应要求系统根据攻击类型、强度动态调整防护策略，打破传统“静态规则”防护的局限性，提升对多变攻击手段的应对能力；可扩展性则需适配不同规模网络环境，无论是中小型企业局域网还是大型跨域网络，均能通过模块扩展满足防护需求。性能指标层面，检测准确率决定攻击识别效果，误报率需控制以避免干扰运维，漏报率需压低以防安全隐患，响应延迟需匹配实时防护需求，资源开销则平衡防护效果与硬件成本[3]。

3.2 系统整体架构

系统整体架构采用分层协同设计。数据采集层作为“入