基于人工智能的网络安全态势感知技术研究

罗　达
中国石油长城钻探工程有限公司工程技术研究院　辽宁盘锦　124010

摘　要：近年来，网络安全问题层出不穷，涉及的范围广、难度深，社会关注度较高，且使用传统人工识别方式已无法满足现阶段防护需求，因此深入研究网络安全态势感知技术意义重大。在各行业关键领域，数据安全通常面临较大威胁，应积极防范网络安全风险，采取有效措施保障数据安全，以有效加强信息化防护能力，减少安全威胁，维护关键技术领域信息安全。基于此，分析基于人工智能的网络安全态势感知结构和关键技术，进而探究基于人工智能的网络安全态势感知技术的具体应用，以期为相关行业人员提供参考。

关键词：人工智能；网络安全；安全态势感知

一、网络安全态势感知的基本理论与技术背景

网络安全态势感知是一种综合性技术手段，旨在通过对网络环境中各类数据与事件进行全方位的感知、分析与预估，达到动态掌握安全状态并提前识别潜在威胁的目的，从而为安全防护决策提供有效支撑。该技术的核心任务是对庞大的网络信息进行实时收集、解析与理解，最终构建出一个整体安全态势图，实现由传统的“被动防守”向“主动识别”及“智能响应”机制转变。

“态势感知”这一理念最初源于军事系统，用于整合战场信息以全面把握敌我局势。转化至网络领域后，其内涵被扩展为对网络空间中攻击路径、系统漏洞以及潜在风险的多层次感知与剖析。目前，网络安全态势感知一般分为三个核心阶段：数据感知与处理、态势理解与评估、态势预测与响应。其中，数据层主要涵盖对网络通信、日志记录及用户行为等方面的采集与处理；态势理解是通过多源信息融合和威胁模型构建，识别出攻击事件的本质特征和发展趋势；在预测阶段，系统依托统计方法与智能算法，对可能出现的威胁进行趋势推演与风险预警，并制定响应策略（如阻断攻击、修复漏洞等）。

从技术发展角度看，近年来以人工智能、大数据处理、云服务为代表的新技术快速兴起，为安全态势感知体系的建设注入了强劲动力。尤其是人工智能技术的加入，使得系统在异常行为检测、模式学习及信息识别方面表现出更高的准确性与效率。包括深度学习、语义分析以及知识推理等先进方法的应用，正逐渐突破以往安全系统的防护瓶颈，推动态势感知能力由静态分析转向智能化推演。

与此同时，国家层面对网络安全工作的重视程度不断提高，相关法律和政策持续完善，为态势感知技术的发展创造了良好的制度基础。像《网络安全法》《数据安全法》等法规的实施，进一步明确了信息保护、追踪溯源和态势分析等方面的要求，也推动着各类关键行业加快构建更为完善的感知系统。

二、网络安全态势感知系统架构与关键技术

1.网络安全态势感知系统架构

一个完整的网络安全态势感知系统通常包括数据采集、数据处理与融合、态势认知与预测、可视化展示四个层级，各模块协同工作，实现对网络安全态势的全面掌握与智能判断。

数据采集层负责收集来自防火墙、IDS/IPS、流量监控、主机行为、漏洞库、恶意代码和威胁情报等多源数据，强调实时性、准确性与多样性。数据处理层则对采集到的信息进行规范化、去噪和关联分析，形成统一的数据视图。

态势认知与预测层通过规则匹配、专家系统和机器学习技术，识别潜在攻击，并进行风险评估与趋势预测，为安全决策提供依据。

可视化展示层将复杂的安全态势以图表形式呈现，帮助管理人员直观了解系统状态、异常事件与攻击路径，提高响应效率。

这种分层结构理清了系统流程，也便于各模块独立优化与协同运行，增强系统的适应性与可扩展性。

2.网络安全态势感知系统关键技术

在搭建网络安全态势感知系统的过程中，若干核心技术的应用对系统的整体性能与实际效果起着决定性作

用，主要涵盖以下几个方面：

大数据技术的支撑：态势感知依赖对体量庞大、来源复杂、结构多样的数据进行处理，因此高效完成数据的采集、预处理、存储与计算是系统稳定运行的基础保障。目前，Hadoop、Spark、Flink等开源平台广泛用于实现分布式计算与实时处理能力，以应对网络数据的高速流动与爆发增长。

人工智能与学习算法的集成：智能化技术是推动系统精准识别威胁的关键工具。借助分类、聚类、深度神经网络等算法，可以辅助发现未知的攻击模式、识别异常行为，并通过持续学习不断调整参数，增强模型对新型风险的适应能力。

多源数据融合方法：该技术旨在整合来自不同网络安全设备及系统平台的分散数据，解决信息孤立和片段化的问题，构建统一的威胁场景视图。通常需要借助语义分析、实体归并、时间序列融合等方法，实现安全信息的协同分析，便于识别完整的攻击过程。

知识图谱与情报驱动分析：通过构建安全知识图谱，可以梳理并关联网络事件之间的潜在联系，从而揭示攻击者行为逻辑与意图路径。与此同时，整合外部威胁情报可拓展系统的视野，使其具备更强的预警和前瞻能力，提升安全策略的精准性。

可视化呈现与交互机制设计：态势感知所产生的复杂数据和分析结果，需通过直观的方式呈现给管理人员。采用基于GIS地图、图关系网络、交互式时间轴等可视化手段，可以帮助使用者快速把握系统运行态势、识别重点风险，从而提升响应效率与处置能力。

以上技术通常不是孤立存在，而是相辅相成、协同集成，构建起具有动态识别、高效分析和快速响应能力的现代化网络安全感知体系。伴随信息技术的进步和威胁场景的持续变化，态势感知系统所依赖的技术框架也将不断演进与完善。

三、网络安全态势感知系统关键技术

1.表征态势指标体系

网络安全态势的直观展现依赖于一套科学且合理的指标体系，这套体系能够对复杂的安全状态进行量化描述与有效表征。指标体系通常基于多维度数据构建，涵盖网络流量状况、主机健康状态、攻击事件的严重等级、关键资产的重要性以及系统漏洞等多个方面。此外，还会结合风险评分、攻击强度和响应速度等动态指标，反映安全态势的实时变化。构建这一指标体系时，必须遵循可观测性、可度量性和可对比性的原则，确保指标既能够全面呈现整个网络的安全状况，又能够突出显示关键节点和潜在的薄弱环节。通过科学的指标设计，管理人员可以更加准确地掌握网络安全整体态势，及时发现风险隐患，从而为安全防护决策和资源分配提供有力支撑。指标体系的合理构建还便于不同时间和不同环境下的态势对比分析，增强安全事件的溯源与评估能力，推动态势感知系统向智能化、精准化方向发展。

2.检测分析与处理技术

网络安全态势感知的核心在于对庞大且多样化的数据进行实时监测、深入分析与高效处理，保障网络环境的安全稳定。该技术体系涵盖多个关键模块，包括异常检测、行为分析、威胁识别以及入侵溯源等。具体手段涉及深度包检测（DPI）、流量指纹识别、协议解析和日志审查等多层次技术，旨在全面捕捉网络中的异常信号与潜在风险。在数据分析阶段，系统通过融合机器学习算法、规则匹配机制和统计建模技术，对网络活动进行详细的行为画像与模式识别，从而准确判断是否存在异常或恶意操作。更重要的是，利用智能化的事件关联与上下文感知分析，能够将表面上分散、孤立的攻击行为串联起来，形成完整的攻击链条。这种关联分析不仅提升了溯源的精确性，也为后续的应急响应提供了科学依据。处理层面，网络安全态势感知系统要求具备一定的自动化响应能力，包括及时隔离异常设备、切断攻击通路、自动生成告警及响应报告等措施，确保一旦检测到威胁能迅速采取防御行动。通过上述综合技术的协同作用，态势感知系统能够实现对网络安全态势的全面把控，提升整体防护效率和准确性，帮助安全管理人员快速决策，有效抵御复杂多变的网络攻击威胁。

3.光谱反病毒查杀技术

光谱反病毒技术是近年来兴起的一种新型恶意代码检测与查杀方法，其核心原理是通过提取文件或进程的“光谱特征”——即程序行为模式与系统调用序列的特征向量，识别未知或变种病毒。不同于传统基于特征码的杀毒机制，光谱反病毒方法更关注程序运行过程中产生的行为特征，并通过比对行为谱图、模式分类与聚类分析等方式进行判别，因此对变异性强、加壳加密的恶意软件具有更高的识别能力。此外，光谱技术通常结合机器学习算法，对样本进行训练与建模，不断提升系统对新型恶意代码的适应性与准确性。在态势感知系统中引入光谱反病毒引擎，不仅能够增强终端防御深度，还能为感知系统提供行为级别的安全数据支撑，有助于整体安全态势的立体化建模与分析。

四、人工智能技术下的网络安全态势感知系统应用

1.实时威胁监测与预警

在复杂多变的网络环境中，人工智能技术极大提升了安全态势感知系统对实时威胁的识别与预警能力。借助机器学习、深度学习等AI方法，系统可对网络数据流、用户行为、访问日志等信息进行持续学习与建模，及时发现异常模式与可疑活动。特别是在面对未知攻击时，AI算法能通过特征提取与异常检测技术，识别出未被签名库覆盖的新型威胁，实现“零日”攻击的初步发现。此外，通过构建基于历史攻击行为的数据模型，系统能够提前预判潜在威胁的可能路径与攻击目标，及时生成预警信息并推送至安全管理终端。这种基于AI的智能预警机制，不仅提高了预警的准确率与时效性，也为安全运营中心提供了更加主动的防御手段，帮助组织在攻击真正发生前采取预防措施，有效降低安全事件的发生概率。

2.恶意软件检测与防护

人工智能技术在恶意软件检测与防护领域的应用，已成为现代网络安全体系中的关键突破点。传统的防病毒方法主要依赖特征码匹配，这种方式面对恶意软件不断变化和快速变异的挑战显得力不从心，难以有效识别新型威胁。相比之下，AI技术通过结合静态分析和动态行为分析，大幅提升了对未知恶意程序的检测能力。静态分析利用机器学习模型对可执行文件中的代码结构和指令模式进行识别，从而发现潜在的恶意特征；动态行为分析则侧重于观察程序运行时的系统调用、文件操作、网络通信等行为，构建行为画像，为判定恶意行为提供依据。深度学习算法的引入，使得系统能够通过大规模样本训练不断优化模型的准确率和适应性，提升对复杂威胁的识别水平。在实际应用中，这类基于AI的恶意软件检测模块通常集成于安全网关、终端防护软件以及邮件过滤系统中，实现多层次、全方位的防护体系。这种协同防御机制能够主动识别和阻断病毒、木马、勒索软件等多种威胁，极大增强了网络环境的安全防御能力。此外，AI技术还支持实时更新和自动学习，使防护系统能快速响应新出现的攻击手法，保持防御的先进性和有效性。随着人工智能技术的不断发展，其在恶意软件防护领域的应用前景愈加广阔，必将推动网络安全防御进入一个智能化的新阶段。

3.自动化响应与修复

人工智能的引入，使得网络安全态势感知系统在应对安全事件时，逐步实现从“人工响应”向“智能响应”的转变。基于AI的自动化响应机制，能够在发现威胁后，迅速触发预设策略进行处理，例如自动封禁异常IP、隔离被攻击主机、终止异常进程等操作，显著缩短了响应时间，降低了人为判断失误带来的风险。同时，通过深度学习与知识图谱等技术，系统还能结合历史事件与规则逻辑，实现攻击链的动态分析与溯源，并对可能存在的系统漏洞进行自动化修复建议或配置加固。此外，自动化修复不仅限于单点处理，还可结合运维系统实现批量更新、策略联动，提升整个网络环境的抗攻击能力。随着AI算法的不断进步，未来自动化响应将朝着更加精细化、自适应方向发展，成为支撑网络安全主动防御的重要支柱。

结束语

随着网络环境日益复杂和威胁手段不断演进，基于人工智能技术的网络安全态势感知系统已成为保障信息安全的重要支撑。通过实时威胁监测、智能恶意软件识别以及自动化响应与修复，系统不仅提升了安全防护的精准度和效率，也推动了从被动防御向主动防御的转型。未来，随着AI算法和大数据技术的持续进步，网络安全态势感知系统将在更大范围、更深层次实现智能化应用，助力构建更加稳健和可信的网络安全防线，保障数字化社会的安全稳定发展。

参考文献

[1]曾进，李皓杰.基于人工智能的网络安全态势感知技术研究[J].信息与电脑（理论版），2023，35（11）：229-232.

[2]李杰.基于人工智能的网络安全态势感知研究[J].通讯世界，2024，31（3）：39-41.

[3]朱珅莹.网络安全态势感知及其应用实践研究[J].软件，2023，44（7）：157-159.

[4]张婷婷.机器学习支持下的网络安全态势感知分析[J].信息与电脑（理论版），2024，36（8）：198-200.

[5]张雨涛.网络安全态势感知系统的应用研究[J].中国信息化，2023（4）：68-69.