基于人工智能的网络入侵检测技术研究*

文◆广东电网有限责任公司东莞供电局　郭孝基　董彩红　梁浩波

引言

网络入侵手段日益复杂，传统机器学习法很难识别入侵行为。因此，应引入现代信息技术提高网络入侵检测技术水平。人工智能技术高速发展，为自然语言处理、语音识别、图像识别提供技术保障，高效处理海量数据信息，以新方法处理多属性入侵数据。在网络入侵检测工作中，应用人工智能技术，有助于提高网络入侵检测准确率，降低漏警率、虚警率。本文基于人工智能，重点讨论网络入侵检测技术的相关问题。

1 人工智能与网络攻击概述

人工智能技术，可以仿真模拟人的思想意识，再现人的思维过程、智能行为。在医药、保险、法律、无人驾驶等领域，人工智能技术的应用频率越来越高。人工智能技术的功能繁多，行为流程复杂，涉及到深度学习、机器学习、认知能力等方面。机器学习无需依赖人工指导，但对学习、推理方法的依赖度高，能够高效完成任务内容。在网络安全防护方面，机器学习模式的应用频率高，能够预测网络不安全行为。

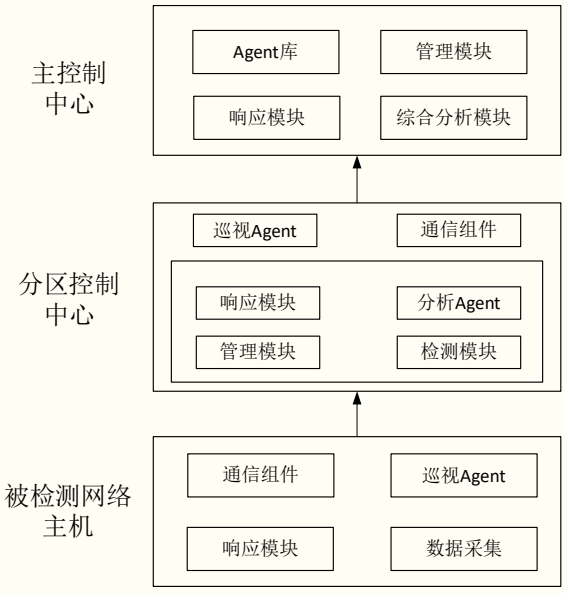

图 1 入侵检测系统硬件结构

当前，云计算供应商建立纳入工具集，以机器学习原理识别恶意攻击、感染宿主，明确网络攻击状态，保障服务器运行正常。基于攻击方式分析，计算机网络攻击包括主动型和被动型。主动型是指不法分子攻击计算机网络防御系统，如拒绝服务、篡改程序、假冒身份等。被动型是指不法分子借助监听技术，对计算机网络的信息流进行窃取，获取重要数据信息。

长期以来，入侵检测技术只能检测已知的入侵行为。但网络入侵技术日益复杂，每日产生的行为、流量数据较多，现有检测技术难以实时监测入侵行为。大部分的网络入侵检测系统，总是以减少虚警率来提高检出率，增加技术人员的工作压力，容易出现信息反馈迟缓情况，对网络安全的影响明显。本文提出的网络入侵检测技术，结合了人工智能

*【基金项目】中国南方电网有限责任公司科技项目“基于 AI 的网络安全态势感知研究与应用”（GDKJXM20230905）。
【作者简介】郭孝基（1986—），男，广东兴宁人，硕士研究生，高级工程师，研究方向：网络安全、数字电网。

技术、神经网络技术，能够快速探测网络入侵行为，减缓网络反馈与响应速度，提高网络信息安全。

2 网络入侵检测技术

2.1 网络入侵检测概述

网络入侵检测系统是指能够阻止不法分子进入，快速发现潜在危险并报警的软件工具。入侵检测系统硬件结构如图 1 所示。按照不同的引擎检测机制，将入侵检测系统分为两种，即特征检测型和异常行为检测型 [1]。

（1）特征检测型。按照特征检测型的特征，在特征数据库内鉴别入侵行为，但是不能对位置、特征值变化进行鉴别。（2）异常行为检测型。参考网络业务特点，合理划分业务类型，探测未知攻击行为。异常行为检测型技术的灵活性更强，且技术扩展空间大。对于特征检测型技术来说，可以快速识别攻击行为，但是却无法鉴别新型攻击行为，所以整体检测率比较低。

2.2 入侵检测工作原理

（1）收集信息。在入侵检测工作中，技术人员应当收集系统、网络、用户行为数据。在不同网络内设置感应器和代理器，获取需求数据，如网络流量、网络日志文件、异常文化变化、异常目录等。（2）分类检测。对于收集的数据、系统、用户行为，传输至检测引擎。按照不同检测机制，检测引擎可以匹配模式、检测异常值、监督学习模型。在分类之前，将模型训练设置为后台运行方式，也可以设置为离线运行方式。（3）决策。当系统检测入侵行为时，控制台参考警报内容，自动生成预定义响应，优化配置防火墙、路由器，更改文件属性、断开网络连接 [2]。

2.3 人工智能在网络入侵检测中的应用

（1）人工智能技术可以实时监测入侵行为，实现检测、响应过程的自动化。此外，在人工智能技术的帮助下，技术人员可以及时发现异常网络活动，积极应对潜在威胁，降低网络攻击伤害，提高网络弹性。（2）人工智能技术可以处理海量数据。在网络安全体系中，技术人员往往要分析大量漏洞信息、网络日志信息，工作量巨大。应用人工智能技术，可实现数据自动化整合与处理，降低了人工成本和工作量，提高了工作效率，为网络入侵检测提供数据依据。

2.4 人工智能的网络入侵检测与防御

网络安全威胁事件频发，且呈现出规模性、隐蔽性特点，严重危害网络安全防护。在人工智能技术指导下，加强网络防御的自主性，提高数据挖掘能力，缩短入侵行为检测到回应的时间，快速识别、检测、处理安全威胁，积极应对不同的网络入侵事件。在探测未知威胁时，人工智能技术的应用效果显著。在人工智能技术的支持下，技术人员能够深度挖掘软件漏洞，准确识别恶意流量和程序，收集威胁信息。

（1）在探测恶意程序时，人工智能可以将病毒样本转化为 2D 图像，之后将图像传输至深度学习网络内，获取 2D 图像判定结果，包括“已感染”“干净”。通过实践论证可知，基于人工智能的恶意程序探测率达到 99.10%，虚警率仅为 1.47%。（2）基于机器学习法，准确检测恶意网络。例如，聚类方法，结合域名生成算法，检测现有的恶意网络，发现新品种。（3）构建威胁情报的知识图谱。基于功能磁共振成像模型，自动提取威胁情报内的实体、关联信息。在知识图谱的辅助下，加快人工提取速度，提高浅层神经网络的识别精度。（4）检测未知密码的恶意数据流，提供对应的算法。如果操作人员无法提取数据包内的数据，则投入 LSTM 数据包，准确识别多类型数据包。（5）基于人工智能技术，建立网络安全平台。结合非监督机器学习、有监督学习方式，自动扫描日志，由管理人员进行验证，将验证结果传输到 AI2 内，可侦破 85% 的网络攻击行为。（6）检测恶意网络流量，如 BoTShark 检测器，基于深度学习原理，全方位检测恶意网络流量。使用卷积神经网络法、叠层自编码机，保证检测过程无需依赖网络流量主体。使用 BoTShark 检测器的识别率达到 90%，召回率为 12%。（7）在检测新型钓鱼邮件时，联合深度神经网络技术、程序算法，对钓鱼邮件进行全方位监测。经过测试后发现，深度神经网络算法的检测正确率超过 90%，实现钓鱼邮件的自动化识别。（8）检测恶意域名时，应用支持向量算法，训练样本为威胁信息，学习威胁信息的特征。人工智能技术的泛化能力非常强，可以减少虚警情况，加大系统控制效果。（9）融合域名生成算法的特征集词汇，提高字符串信息的使用率。此种方法的特征抽取性能、分类性能均比较高，能够减少数据不均衡的影响。（10）通用型漏洞检测方法。此种方法和缺陷检测法的差别非常大，无需采集、清理、标记样本，即使功能类似，也会出现不同的代码。在开放源码软件内，通用型漏洞检测法可发现隐藏缺陷 [3]。

3 基于人工智能的网络安全管理

3.1 发现和处理异常事件

人工神经网络系统的分辨能力较强，将其引入到网络安全管理中，可以准确识别入侵行为，适应能力非常强。人工神经网络系统，具备较强的学习能力、理解能力，可以快速识别、存储数据，检测质效高，特别是病毒入侵检测。利用模糊识别系统，快速定位系统隐藏病毒，并向系统作出响应，保障网络系统的安全运行效果。当网络系统遭受攻击时，以多元方式发出警报。网络体系内包含大量安全设备，以报警灯、窗口报警灯方式发出警报，数据库可以自动存储报警数据。

3.2 智能检测数据流量

数据流量与体积相关，不管是数据上传或下载，都会产生流量波动。当数据体积较大时，流量浮动也比较大。人工智能技术借助数据流量与体积的关系，智能检测数据流量，加大数据安全保障力度。病毒往往隐藏在数据内部，用户下载携带病毒的数据时，流量消耗非常大，当人工智能检测到异常数据流量时，就会断开数据传输，向数据库提交内容检索申请，对照数据库内的数据，判断下载数据的安全性。如果为风险数据，人工智能就能向数据库上传数据来源、内容、特征，作为后续学习内容。部分网络终端处于开放状态，病毒会私自连接网络开展非法活动。当病毒与网络连接后，流量消耗大，人工智能技术能检查终端设备使用情况，如鼠标、键盘、触控设备等，若存在异常数据消耗，可以自动限制不良行为。

3.3 智能隔离与控制

在预定义安全对策下，人工智能防火墙能够对内外网络进行监控。人工智能防火墙，包含身份识别技术、状态监测技术、包过滤技术。例如，包过滤技术旨在选择网络层的数据包，参考系统的运行状态，提前设置过滤逻辑，提高数据包内容的安全性。电子邮件成为常用的信息传输载体，应用人工智能防火墙监控电子邮件，检验邮件信息与内容，查看其是否携带病毒。如果发现潜在病毒，立即隔离并控制邮件，减少网络信息的安全隐患。

4 人工智能的网络入侵检测发展趋势

网络入侵威胁的变化颇多，为了保障网络安全防御效果，必须提高网络入侵检测的智能化水平。在未来发展中，可通过以下措施保障网络安全。

（1）在网络入侵检测工作中，深度学习、强化学习技术将成为重要趋势。在处理大规模数据，对复杂模式进行识别时，深度学习发挥出显著作用。通过强化学习方式，积极化解智能化威胁，修补网络漏洞。将强化学习、深度学习技术结合在一起，建立智能化的网络安全系统，主动应对攻击行为。（2）对抗性机器学习研究的发展趋势。不法分子以新型技术欺骗机器学习模型，故应加强模型的抗攻击性，如改进模型的鲁棒性、开发对抗性训练技术、设计安全模型架构等。（3）大数据、物联网安全的发展趋势。物联网设备的普及率提升，网络攻击面会持续扩大，因此应建立健全智能监测机制、防御机制，为物联网设备、数据提供保护。在大数据技术支持下，准确识别物联网设备的潜在威胁、异常活动。（4）隐私保护、合规性研究的发展趋势。在网络入侵检测、防御机制中，大量个人数据被征用，因此要引入科学的隐私保护措施，遵守法律要求。

综上所述，网络入侵检测、防御的发展趋势，将以智能化作为核心，联合强化学习技术、深度学习技术、对抗性机器学习技术，加大网络安全的保护力度。在未来发展中，网络系统将会出现新的攻击程序及行为，因此对于网络安全的研究与创新，必须朝着数字化、安全化趋势发展。

结语

人工智能技术的优势与价值显著，可以自主学习网络恶意攻击行为，搭建多元化的防护系统，全方位找寻网络系统存在的安全隐患，隔离和控制不良入侵行为。在人工智能技术的支持下，网络安全水平得到明显提高，可快速识别响应未知威胁和已知威胁。在未来发展中，网络入侵检测的智能化水平持续提高，将助力积极应对隐藏的网络攻击行为。

引用

[1] 董卫魏,王曦,钟昕辉,等.基于人工智能技术的轻量级网络入侵检测系统设计[J].现代电子技术,2024,47(5):108-111.

[2] 史进.基于改进决策树的软件定义网络的入侵检测技术应用研究[J].网络安全技术与应用,2023(11):38-41.

[3] 沈溶溶.基于人工智能技术的计算机网络入侵检测方法设计[J].长江信息通信,2023,36(5):127-129.