基于人工智能的信息网络安全态势感知技术分析

陈　晗
浙江海瑞网络科技有限公司　浙江湖州　130000

摘　要：受经济快速发展的推动下，我国现代互联网技术也有所提高，并迎来了信息时代。如今，信息安全非常重要。由于是一个相对开放的环境，网络上存在着很多方面隐患，尤其是信息网络安全。因此，进一步增强信息网络安全的方法也成为公众关注的焦点。

关键词：人工智能；信息网络安全态势；感知技术

随着网络黑客技术的不断发展，网络的安全性一直备受争议，所面临的潜在威胁也在不断增加。传统的被动防御体系（入侵检测系统、防火墙、防病毒软件等）已经满足不了人们对网络安全的需求。人们需要在很长一段时间内提供足够的网络安全。电子网络安全技术的出现，为保障信息网络安全开辟了新的机遇。

一、态势感知概念

它是具有动态和整体能力的大数据，可以根据特定时间和地点的环境识别安全风险。您可以有效地识别、理解、评估、处理并最终针对安全威胁采取行动和做出决策。这个概念最早是在军事领域提出的，主要包括三个层次的理解和一系列的预测。随着互联网的发展，这个概念已经进一步蔓延。并且上升到网络态势感知，可以大规模的对网络环境中可能引起网络态势发展的诸多元素进行获取、理解、显示。近年来，计算机和通信技术发展迅猛，网络应用的数量不断增加，其应用水平和潜在风险不断增加。尤其是一些网络病毒、黑客等构成严重威胁。通过这种方式，网络和技术应用程序可以有效地识别风险并进行最终处理[1]。

二、基于人工智能的信息网络安全态势感知关键技术

1.表征态势的指标体系

表征态势的指标体系是进行态势感知的依据，例如决定去医院或看医生时选择什么。您需要创建一个全面而简洁的指标系统。目前的指标主要包括三个指标：基础运行指标、网络脆弱性指标和网络风险指标。

（1）基础运行指标

主要性能指标是当前网络性能、传输设备负载和表征物流环境的几个指标。该指标不直接反映安全问题，而是间接影响基本运行条件下的安全状态。例如，如果主网流量非常大，则存在大流量攻击后网络崩溃的风险。基本流量直接影响网络的抗冲击能力。

（2）网络脆弱性指标

网络脆弱性指数显示了整个网络的漏洞和脆弱性的情况。网络脆弱性指标通常包括：关键设备健康指数、DNS服务器健康指数、核心路由器健康指数、核心交换机上的负载。

（3）网络威胁指标

网络威胁指示器显示网络上各种威胁代理的位置。威胁状况主要包括各种网络攻击和各种潜在威胁的频率和规模。僵尸网站、垃圾邮件、网络钓鱼和恶意软件、病毒等都是潜在威胁。网络威胁指标通常包括攻击强度指标（一次网络攻击事件的严重程度表示发生多次攻击事件、网络故障的可能性大）、入侵事件指数、挂马密度指数、仿冒网站密度指数等。

2.预测态势算法

目前，流程态势感知采用的算法基本上是根据开发情况和工作历史状态的测试结果进行验证的预测位置人工智能算法。目前态势感知过程中使用的位置预测算法主要由人工神经网络法和特殊预测法两种方法组成。首先建立的预测模型通常包括技术分析BF网络、BP网络，可以起到更可预测的作用。但是，这种神经网络算法完全符合应用程序本身的局部最优解。熟练预测技术是一种以知识和经验设计的智能编程系统。在现实生活中，这些专家模拟人类思维，以分析现实生活中的复杂问题。这不仅有效地降低了计算复杂度。同时，根据人的思想做出不同的决定有很多好处。该算法具有很强的针对性，我们需要依靠丰富的知识和丰富的数据才能将其变为现实。但是，网络是一个比较大和复杂的空间，由于不完全满足上述条件，预测效率是有限的。因此，必须将这种方法的应用添加到电力系统的有效运行条件中，以便在经过充分和详细的调查后选择适用于电力系统的算法来保证预测的准确性[2]。

三、基于人工智能的信息网络安全态势感知具体技术

1.数据采集阶段

您可以收集防火墙日志、互联网日志服务等信息，并提供基础数据进行分析。采集到的数据需要被系统识别并通过云服务器进行更新。随着网络信息量的增长，收集流量镜像数据变得困难，可以使用多种技术方法来方便数据收集。四大核心技术：一是端口匹配技术，当前的网络发展时代跨越了几十年。在网络协议不断发展的过程中，已经形成了几种通用的协议规范。对于用于不同类型协议的端口，这些规范相对灵活。因此，根据这种现象和相关标准，可以获得快速的端口识别和较高的检测效率。另一个是流量测量技术。该技术有两种检测方式：分别针对标准协议流量与未公开协议流量。前者所包含的命令、状态迁移机制等信息都有明确的专有字段和状态，虽然系统可以进行直接准确的识别，而后者则需要通过逆向工程对协议机制进行系统分析，对特征字段进行解密后方能识别该流量。三是自动链接技术。为了克服一个通道提供所有功能的系统的缺点，许多现有协议使用动态协商的端口来传输数据。确认电子邮件中的信息会自动链接到下载链接。执行数据恢复。四是行为分析法。该技术主要针对难以恢复的特定数据流量。对于这个流量，我们使用流量和返回流量等统计特征来分离数据流，而不是链接数。

2.数据预处理阶段

由于这种识别技术是基于证据开发的，因此可以使用大数据来降低处理后续数据以处理收集到的信息的复杂性。该技术主要利用大数据技术的流结构。大数据技术具有处理速度高、可扩展性强、并发处理能力强等优势。典型的预处理活动包括：首先是数据集成。第一是数据归一，在Stream流中，系统将所收集的包括日志信息、数据流量等内容在内的数据进行统一处理，并作为进一步分析系统的数据元素。第二个是知识库的链接。通过将信息数据库链接到知识库，您可以获得分析公司安全状况所需的支持信息。它还旨在为系统的进一步分析提供一个数据库。第三种是数据集成，系统根据计算机分析机器的预定义事件处理结构来集成数据。通过将所有系统输入事件集成到处理过的历史数据的内容中，针对数据流中的任何异常情况分析该性能，从而引起警报。

3.数据存储与检索阶段

由于信息网络上存储的信息量巨大，所以系统在对大量数据进行检索时一般可以借助搜索引擎来完成，这些数据可用于执行分布式全文搜索和公司云计算。环境非常适合。在特定的搜索模式下，系统平台对信息进行处理和展示，然后将数据存储在分布式搜索引擎索引文件中，按照时间、名称、内容等对每种数据类型进行排序，然后按回车键。索引支持数据收集操作的导出字段。此外，在分布式文件系统中将索引存储为多个切片和多个副本，可以有效地近似查询最后输入的数据，以类似的方式获取查询信息。信誉证明可以保证真实性。这减少了在辅助系统上索引TB级数据所需的时间，并显着提高了索引性能。

4.检测分析与处理阶段

即使按照上述步骤操作后，您仍应使用各种方法对数据进行彻底分析和研究，以识别潜在风险。有四种主要的应用技术。其中之一是用于检测恶意代码的智能技术。通过对一些常见程序和恶意软件的分析比较，发现了这两个程序的内在特征，并从中构建了机器学习模型。获取恶意软件检测模板并运行恶意软件扫描。二是广谱杀毒检测器，增强了独创的病毒检测技术，提高了稳定性。三是机器学习技术，提供强大的机器学习能力。将信息数据传输到分析仪器手册，以获得分析的原始数据。四是自动数据处理。电子技术虽然是基于人工智能的，但它仍然以人为中心，需要使用自动数据处理来分析数据。通过将潜在风险与人工干预相结合，可以最大限度地提高测试结果的准确性[3]。

四、结束语

近年来，我国对网络安全技术进行了研究。随着人工智能的出现，他在电子技术研究中发挥了重要作用。电子网络技术基于互联网基础信息和关键信息系统的创建和保护。我国电子网络安全技术尚处于研究阶段，大部分领域为学术研究领域。网络安全的本质仍然没有改善。数据集成技术、数据挖掘技术、数据模式识别技术还处于起步阶段整体而言，距离产品化还相差甚远。

参考文献：

[1]胡庆伟.对基于人工智能的信息网络安全态势感知技术分析[J].网络安全技术与应用，2020（05）：149-150.

[2]王小鸿.基于大数据和人工智能技术的信息安全态势感知系统研究[J].大众标准化，2019（14）：18+20.

[3]刘雅娟，胡荣.基于大数据和人工智能技术的信息安全态势感知系统研究[J].中小企业管理与科技（中旬刊），2019（09）：153-154.