人工智能在网络安全事件溯源中的应用

湛鹏文
青海省中国特色社会主义理论体系研究中心　青海　西宁　810001

摘　要：本文聚焦人工智能在网络安全事件溯源中的应用。概述了人工智能，涵盖其定义、涵盖领域及发展现状。阐述网络安全事件溯源的重要性，如维护法律、保障企业运营与国家安全等。分析传统溯源方法面临的挑战，包括数据复杂、人工分析低效及难以应对新型攻击。重点探讨人工智能在数据收集处理、异常检测、事件轨迹重建等方面的应用，并分析其优势与挑战，为网络安全事件溯源提供新思路。

关键词：人工智能；网络安全；事件溯源

1 人工智能概述

人工智能（ArtificialIntelligence，AI）是一门致力于研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的新技术科学。它试图让计算机具备像人类一样的感知、理解、学习、推理和决策等能力。人工智能涵盖多个领域，如机器学习、深度学习、自然语言处理、计算机视觉等。机器学习通过算法让计算机从数据中学习模式和规律，无需显式编程；深度学习作为机器学习的分支，利用深层神经网络处理复杂的模式识别任务；自然语言处理使计算机能够理解、生成和处理人类语言；计算机视觉则赋予计算机“看”的能力，实现对图像和视频的分析与理解[1]。近年来，随着计算能力的提升、数据量的爆炸式增长以及算法的不断创新，人工智能取得了飞速发展，在医疗、金融、交通、教育等众多领域得到广泛应用，为解决复杂问题提供了新的思路和方法，也为网络安全领域带来了新的变革契机，尤其在网络安全事件溯源方面展现出巨大潜力。

2 网络安全事件溯源的重要性

网络安全事件溯源在当今数字化时代具有不可忽视的重要性。第一，从法律层面看，在发生网络安全事件后，溯源能够确定攻击者的身份和行为，为执法机构提供关键证据，有助于将犯罪分子绳之以法，维护法律的尊严和网络安全秩序。第二，对于企业而言，溯源可以帮助企业了解攻击的来源、手段和目的，从而评估自身网络系统的安全漏洞，采取针对性的措施进行修复和加固，防止类似事件再次发生，保障企业的正常运营和业务连续性。第三，溯源有助于企业挽回经济损失。许多网络安全事件会导致企业数据泄露、业务中断，给企业带来巨大的经济损失。通过溯源，企业可以追踪数据流向，尽可能减少数据泄露的范围，同时采取措施防止攻击者进一步利用泄露的数据进行非法活动。第四，网络安全事件溯源对于维护国家安全也至关重要。一些网络攻击可能针对国家关键基础设施，如能源、交通、通信等领域，溯源能够及时发现并应对这些威胁，保障国家的安全和稳定。

3 传统溯源方法面临的挑战

3.1 数据量大且复杂

随着互联网的普及和企业信息化程度的提高，网络中产生的数据量呈爆炸式增长。这些数据不仅数量庞大，而且来源广泛、格式多样，包括网络流量数据、系统日志、应用程序日志等。传统溯源方法在处理如此大规模且复杂的数据时，面临着巨大的困难。而且，不同来源的数据可能存在格式不统一、语义不一致等问题，增加了数据整合和分析的难度。数据的动态性也给溯源带来了挑战，网络环境不断变化，数据实时更新，传统方法难以实时处理和分析这些动态数据，从而影响了溯源的及时性和准确性。

3.2 人工分析耗时长、效率低

传统溯源方法往往依赖人工分析，安全专家需要仔细审查各种数据，寻找异常行为和攻击线索。然而，人工分析不仅耗时费力，而且效率低下。面对海量的数据，人工分析难以做到全面、细致，容易出现遗漏和错误。同时人工分析的速度远远跟不上网络攻击的速度，在攻击发生后，无法及时进行溯源，导致攻击者有足够的时间销毁证据或继续实施攻击。人工分析还受到安全专家个人经验和知识水平的限制，不同专家的分析结果可能存在差异，影响了溯源的可靠性。

3.3 难以应对新型攻击手段

随着网络技术的不断发展，攻击者的手段也日益复杂和多样化，新型攻击手段层出不穷，如零日漏洞攻击、高级持续性威胁（APT）攻击等。这些新型攻击手段具有隐蔽性强、难以检测的特点，传统溯源方法往往

难以应对。传统方法主要基于已知的攻击模式和规则进行检测和溯源，对于新型攻击缺乏有效的识别和应对能力。攻击者可以利用未知的漏洞或采用创新的攻击方式，绕过传统的安全防护机制，使得传统溯源方法无法及时发现和追踪攻击来源，给网络安全带来了严重威胁。

4 人工智能在网络安全事件溯源中的应用

4.1 数据收集与处理

在网络安全事件溯源中，数据收集与处理是基础且关键的环节，人工智能技术在此方面发挥着巨大作用。借助先进的技术手段，能够实现对多源异构数据的自动收集。通过在网络中广泛部署各类传感器和监测设备，如同布下了一张严密的监控网，可实时收集网络流量、系统日志、用户行为等海量数据[2]。网络流量数据反映了网络中数据的传输情况，系统日志记录了系统和应用程序的运行状态，用户行为数据则体现了用户在系统中的操作习惯。收集到的数据往往存在噪声、缺失值以及格式不统一等问题，人工智能利用机器学习算法对这些数据进行清洗、去噪和标准化处理。同时人工智能还能对数据进行特征提取，从海量的原始数据中挖掘出有价值的信息，如网络连接的频率、用户登录的时间规律等，这些特征信息为后续的溯源工作提供了坚实的基础，有助于更准确地识别和分析网络安全事件。

4.2 异常检测与威胁识别

人工智能在网络安全事件溯源的异常检测与威胁识别方面展现出了显著优势。基于机器学习和深度学习算法，能够构建出精准的正常行为模型。通过对大量正常网络行为数据的学习和分析，该模型可以深入理解网络在正常运行状态下的各种模式和规律。一旦出现与正常行为模式不符的异常行为，系统便能迅速识别出来。以深度学习中的神经网络模型为例，它可以对网络流量进行细致的分类和预测。通过对网络流量的特征提取和分析，神经网络模型能够判断网络连接是否异常、数据传输是否存在风险。人工智能还能结合威胁情报，对已知的攻击模式和特征进行学习和识别。威胁情报包含了各种已知攻击的详细信息，如攻击手段、攻击目标等。通过对攻击行为的特征提取和分析，能够准确判断攻击的类型和来源，为溯源工作提供关键线索，帮助安全人员快速定位攻击者。

4.3 事件轨迹重建与关联分析

在网络安全事件溯源中，重建事件轨迹和进行关联分析是揭示攻击真相的关键环节，人工智能技术为此提供了强大的支持。利用收集到的丰富数据，人工智能可以通过图算法和关联规则挖掘等方法，重建攻击事件的完整轨迹。图算法能够将网络中的各个节点（如系统、设备等）和边（如网络连接、数据传输等）以图的形式表示出来，通过分析图的结构和关系，可以清晰地展示攻击者在不同系统和设备之间的活动路径。关联规则挖掘则可以从大量的数据中发现事件之间的潜在联系[3]。如果发现某个系统在特定时间点出现了异常登录行为，随后又发生了敏感数据的传输，那么就可以推断出攻击者可能通过该异常登录行为进入了系统，并窃取了敏感数据。同时对多个安全事件进行关联分析，能够找出事件之间的内在联系和潜在关系，揭示攻击者的攻击策略和目标。通过对多个事件的关联分析，安全人员可以了解到攻击者是采用何种手段进行攻击的，其最终目标是什么，从而为制定有效的防御策略提供依据。

4.4 自动化响应与策略制定

人工智能在网络安全事件溯源中能够实现自动化响应和策略制定，大大提高了网络安全防护的效率和及时性。当检测到安全事件时，系统可以根据预设的规则和算法，自动采取相应的措施。同时基于对安全事件的分析和溯源结果，人工智能可以自动生成针对性的安全策略。例如，通过对攻击行为的分析，了解到攻击者是利用了某个系统的漏洞进行攻击的，那么系统可以自动调整防火墙规则，阻止类似攻击的再次发生；或者更新入侵检测系统的签名库，提高对新型攻击的检测能力。这些自动生成的安全策略能够及时有效地提高网络系统的安全防护能力，减少安全事件的发生和损失。

4.5 可视化与报告生成

为了方便安全专家对网络安全事件溯源结果进行分析和决策，人工智能技术将复杂的溯源过程和结果以可视化的方式呈现出来，具有极其重要的意义。通过图表、图形等多种形式，人工智能能够直观地展示攻击事件的轨迹、关联关系等信息。例如，使用时间轴图表可以清晰地展示攻击事件发生的时间顺序，让安全专家了解攻击的发展过程；利用网络拓扑图可以直观地呈现攻击者在不同系统和设备之间的活动路径，帮助安全专家快速定位攻击源头。人工智能还可以自动生成详细的溯源报告，报告中包括攻击事件的描述，如攻击发生的时间、地点、影响范围等；溯源过程，即如何通过数据收集、分析和关联等手段找到攻击来源；攻击来源，明确攻击者的身份或攻击源的地址；以及影响范围，评估攻击对网络系统和业务造成的损失等。这些详细的溯源报告为安全管理和决策提供了有力支持，安全专家可以根据报告中的信息制定更加科学合理的安全策略，提高网络系统的安全性。

5 人工智能在网络安全事件溯源中的优势与挑战

5.1 提高溯源效率与准确性

如今，网络环境复杂多变，产生的数据量呈爆炸式增长，传统方法在处理这些海量数据时往往力不从心，耗时费力且容易出错。而人工智能能够快速高效地处理这些数据，通过先进的算法和模型，自动对数据进行筛选、分析和挖掘，迅速识别出其中的异常行为和攻击线索。以往需要人工花费数天甚至数周才能完成的数据分析工作，人工智能可能在短时间内就能完成，大大缩短了溯源的时间，使安全人员能够更快地采取应对措施，减少损失。同时，基于机器学习和深度学习算法构建的模型具有自我学习和优化的能力。随着不断接触新的数据和攻击案例，模型能够自动调整参数，提高对各种攻击行为的识别准确率。它能够区分正常行为和异常行为的细微差别，减少误报和漏报的情况。误报会让安全人员浪费时间和精力去处理虚假警报，漏报则可能导致真正的攻击被忽视，而人工智能的应用有效避免了这些问题，从而显著提高了溯源的准确性，为网络安全提供了更可靠的保障。

5.2 降低人工干预需求

传统网络安全事件溯源方法高度依赖大量的人工分析，安全专家需要花费大量时间和精力对各种数据进行审查和分析，这不仅效率低下，而且容易出现人为错误。而人工智能的出现，实现了对网络数据的自动化处理和分析，极大地减少了对人工的依赖。人工智能系统可以不知疲倦地对网络数据进行实时监测和分析，快速发现潜在的安全威胁，并自动进行初步的溯源工作。这使得安全专家能够将更多的时间和精力投入到对复杂问题的深入分析和决策上，提高了整体工作效率。人工智能系统可以24小时不间断地运行，持续监测网络数据。在人工分析中，由于人的精力和注意力有限，可能会出现疏忽和延误的情况，导致一些安全事件未能及时发现和处理。而人工智能系统不存在这些问题，它能够及时捕捉到每一个异常信号，并迅速做出响应，确保网络安全事件得到及时处理，有效降低了因人为因素导致的安全风险。

5.3 增强对新型攻击的识别能力

在网络攻击手段不断演变的今天，新型攻击层出不穷，给网络安全带来了巨大挑战。人工智能凭借其强大的学习能力，能够通过学习大量的数据和攻击样本，发现新型攻击的特征和模式。与传统的基于规则的检测方法相比，传统方法往往只能识别已知的攻击模式，对于新型攻击则束手无策。而人工智能具有更高的灵活性和适应性，它不依赖于预先设定的规则，而是通过对数据的分析和学习，自动识别出异常行为和潜在威胁。然而人工智能在网络安全事件溯源中也并非一帆风顺，人工智能模型的训练需要大量的高质量数据，但网络安全数据的获取和标注往往存在困难[4]。数据获取可能受到隐私保护、数据共享限制等因素的影响，而数据标注需要专业的知识和技能，成本较高。这可能导致模型训练不充分，影响溯源效果。另外，人工智能算法的可解释性较差，安全专家难以理解模型的决策过程和依据，在溯源过程中可能面临信任问题。同时攻击者也可能利用人工智能技术进行攻击，如生成对抗样本欺骗检测模型，给网络安全带来了新的挑战。因此在应用人工智能进行网络安全事件溯源时，需要充分考虑这些挑战，并采取相应的措施加以应对。

结束语

人工智能为网络安全事件溯源带来了新的机遇与变革，在提高溯源效率、降低人工干预、增强新型攻击识别能力等方面展现出显著优势。然而，其应用也面临数据获取标注困难、算法可解释性差及可能被攻击者利用等挑战。未来，需持续探索创新，解决现存问题，充分发挥人工智能在网络安全事件溯源中的作用，以更好地保障网络安全，维护社会稳定和企业利益。

参考文献

[1]雷之宇,孙皓,邹悠珍,等.人工智能网络安全领域专利地图分析[J].网络安全技术与应用,2024,(08):113-115.

[2]于汇远.人工智能技术在大数据网络安全策略中的应用[J].电子技术,2023,52(10):234-235.

[3]邵元发.人工智能技术在计算机网络安全中的应用[J].造纸装备及材料,2023,52(10):112-114.

[4]尚学艳.人工智能在网络空间安全中的应用策略[J].中国建设信息化,2023,(23):70-73.