文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

基于人工智能的网络攻击检测方法

朱磊
武警德州支队
DOI:10.12238/acair.v3i1.11897

[摘　要] 本文先探讨了人工智能在网络攻击检测中的作用,然后分析了基于人工智能的网络攻击检测面临的难题,包括数据的复杂性、高速网络环境下的实时检测挑战、不同攻击手法导致的检测难度增加以及面对新兴攻击的模型升级难题。最后,本文提出了基于人工智能的网络攻击检测方法,包括数据预处理、轻量级深度学习模型、多模态学习、深度神经网络、迁移学习和联邦学习等技术,以期提高网络攻击检测的性能和适应性。
[关键词] 人工智能；网络攻击检测；数据复杂性
中图分类号：TP18　文献标识码：A

Network attack detection method based on artificial intelligence

Lei Zhu
Dezhou Detachment of Armed Police

[Abstract] This paper first discusses the role of artificial intelligence in network attack detection, and then analyzes the challenges of network attack detection based on artificial intelligence, including the complexity of data, the real-time detection challenges in high-speed network environment, the increased difficulty of detection caused by different attack methods, and the problem of model upgrading in the face of emerging attacks. Finally, this paper proposes a network attack detection method based on artificial intelligence, including data preprocessing, lightweight deep learning model, multi-modal learning, deep neural network, transfer learning and federation learning, etc., in order to improve the performance and adaptability of network attack detection.
[Key words] artificial intelligence; Network attack detection; Data complexity

引言

随着互联网的普及和网络技术的飞速发展,网络攻击的手段和规模也在不断演变和扩大,给全球网络安全带来了前所未有的挑战。传统的网络攻击检测方法往往依赖于预定义的规则和签名,难以应对日益复杂和多变的网络威胁。人工智能技术,尤其是机器学习和深度学习,因其强大的数据处理能力和模式识别能力,为网络攻击检测提供了新的解决方案。本文旨在探讨人工智能在网络攻击检测中的应用,分析当前面临的挑战,并提出相应的解决方法,以期为网络安全领域提供参考和启示。

1 人工智能在网络攻击检测中的作用

随着信息技术的迅猛发展,网络安全问题已经成为全球面临的重要挑战。传统网络安全防御手段已逐渐暴露出缺陷,不能应对越来越复杂多样的网络攻击。人工智能(AI)的出现,为网络攻击的侦测带来了创新的策略。人工智能技术特别是机器学习与深度学习在大数据分析,模式识别与异常检测领域所具有的巨大能力使得它们在网络攻击检测领域显示出了极大的潜能。通过自动分析学习大量网络流量数据,AI可以检测出可能存在的攻击行为,及时报警,大大提高攻击检测准确性与响应速度。相较于传统的基于规则检测方法,人工智能可以依据实时数据动态适应并持续优化检测策略以增强系统自我学习和攻击识别能力。在此基础上,人工智能可以在实时检测时迅速发现新的攻击模式,大大提高网络安全防护灵活性与有效性。

2 基于人工智能的网络攻击检测难题

2.1网络攻击数据的复杂性、稀疏性和不平衡性

基于人工智能检测网络攻击时,以数据为核心动力。但是网络攻击数据自身的复杂性,稀疏性以及不平衡性等特点对数据分析以及模型训练都提出了很大挑战。网络攻击数据类型多样,攻击手段复杂多样,往往呈现出多种隐蔽和非线性关联等特点,给大规模数据集的有效识别带来了极大的难度。不同种类攻击数据会以不同方式呈现,这就使得检测算法必须有足够的泛化能力以适应多种场景。另外,网络攻击数据通常表现出稀疏性,

也就是说多数网络流量正常,仅有少量攻击流量存在。该数据分布不均衡性使训练时模型易受正常数据干扰而降低攻击数据检测精度。数据不平衡问题往往使训练好的模型倾向于对正常行为进行检测,忽视了少量攻击行为从而影响了检测性能。为改善检测效果,在对此类不平衡数据的处理过程中,需对模型进行有效调整与优化。由于攻击数据比较少,并且其特性通常表现出高度复杂性与多样性,也就决定了人工智能模型要在海量非攻击数据上与弱攻击信号相区别,对于模型复杂度与计算资源都有很高的需求。

2.2高速网络环境下的实时检测挑战

随着网络带宽越来越大,尤其是5G及未来6G网络环境驱动,网络流量速度及数据量有了很大增长。这一高速网络环境对实时检测提出很大挑战。在该环境中攻击者能够使用高网络带宽实现大范围和快速攻击,而传统基于规则检测方法通常不能紧跟数据处理速度,造成网络安全系统反应落后,不能及时的发现并处理攻击行为。以人工智能为基础的检测方法尽管具有精准度等优点,但是面对高速大流量网络环境,数据处理速度快,实时性强等问题依然是它所面临的主要挑战。AI模型进行实时检测时,需要对海量复杂数据进行处理,实时性与高效性成了限制该模型性能发挥的主要原因。以深度学习模型为例,其数据处理与特征提取通常需要很长的时间来训练与推理,这样会导致系统出现响应延迟而不能及时检测出攻击。

2.3不同攻击手法导致的检测难度增加

在网络攻击手段不断革新的今天,攻击者已经不满足于单纯的恶意攻击,而开始使用更复杂多变的攻击方式。这些创新的攻击策略,如零日攻击、分布式拒绝服务攻击(DDoS)和社交工程攻击等,都为网络攻击的检测带来了额外的挑战。很多现代攻击手法通常隐蔽性强,智能性高,攻击者采用加密,伪装以及变种的手法,这就使攻击行为很难通过传统基于特征匹配检测方法来识别。传统方法一般依靠攻击行为已知特征进行异常流量检测,但是对新型攻击而言,它们可能会截然不同,甚至不易被人为察觉。不同攻击手法的攻击方式及攻击目标都不相同,要求检测模型能识别并分辨出多种不同的攻击方式,使得模型训练变得更加困难。对AI系统来说,为了探测到这些攻击就必须从海量的正常流中抽取攻击特征并能精确地对各类攻击进行分类。不同攻击的复杂性与变动性决定了AI模型在面对多样化攻击策略与技巧时必须要有很高的灵活性与适应性。

2.4面对新兴攻击的模型升级难题

网络攻击日新月异的发展变化,使基于人工智能网络攻击检测模型需要不断升级与调整才能适应新型攻击方式。但在攻击模式不断改变的情况下如何对模型进行高效的更新与升级已成为难以解决的难题。人工智能模型一般需要从海量历史数据中训练而成,但是伴随着新的攻击手法不断产生,已有模型常常很难应对从未见过的攻击种类。该模型在此条件下可能存在识别率较低或误报率较高等问题,使模型在应用时效果较差。模型的更新一般都要对新攻击数据重新采集并标记后再进行模型训练。但是网络攻击类型与模式变化很快,新型攻击形式很可能会在短期内大量出现,从而使传统人工干预式模型更新过程变得捉襟见肘。另外,AI模型训练所需计算资源大、耗时长,面对瞬息万变的攻击场景,常规训练周期不一定能达到实时更新要求。

3 基于人工智能的网络攻击检测方法

3.1应用数据预处理、数据增强及生成对抗网络(GAN)以提升数据质量

由于攻击数据具有稀缺性、不平衡性等特点,因此对数据进行预处理与增强对于模型训练起着至关重要作用。数据预处理采用去除噪声,填补缺失值以及归一化的方法来保证数据能得到AI模型的正确认知与处理。在实践中,网络攻击数据相对匮乏,常规训练数据通常不足以建立有效的检测模型。所以数据增强技术非常重要。数据增强利用产生新攻击数据样本来扩大原始数据集大小以增强模型泛化能力。此外,生成对抗网络(GAN)作为一项新兴的人工智能技术,具有通过对抗性训练来生成高品质攻击数据的能力,从而进一步增强了数据集的多样性和全面性。GAN在生成器与判别器之间训练对抗,使产生的攻击样本接近于实际攻击行为,从而为AI模型的建立提供了更多的数据支持。使用GAN产生的攻击样本进行攻击,该模型可以学习更多的各种攻击特征以提高检测精度。对数据进行预处理与增强,既能促进数据质量的提高,又能有效地缓解数据不平衡现象,从而为网络攻击检测工作提供更可靠的数据支持。

3.2利用轻量级深度学习模型与在线学习算法实现快速响应

传统深度学习模型一般含有大量参数且计算繁杂,造成响应速度慢。针对这一难题,研究人员提出一种轻量级的深度学习模型。通过减少网络结构中的层数,精简参数量以及优化计算方式等措施,这类模型可以显著提高模型推理速度,同时又能保证数据的准确性。轻量级深度学习模型非常适合在高速网络环境中执行实时检测任务,可以快速响应和及时发现攻击行为。另外,在线学习算法还提供动态更新模型的功能,使系统可以在多变的网络环境下不断地学习与完善。利用在线学习的方法,AI模型可以在实时数据中持续地抽取出新的攻击特征和及时地更新模型权重以增强新型攻击检测能力。该方法规避了传统训练方式耗时长,计算成本大等问题,使网络安全系统面临大规模,复杂的攻击时仍能保持高度实时性与准确性。所以将轻量级深度学习模型和在线学习算法相结合可以对网络攻击检测给出快速响应。

3.3使用多模态学习和深度神经网络实现对多种攻击类型的识别

传统基于单个数据模态进行检测的方法通常受限于数据类型及复杂度等因素,很难对复杂多变的攻击方式进行全面且高效的识别。伴随着人工智能科技的持续进步,多模态学习(Multimodal Learning)已逐步崭露头角,成为网络安全研究的一个核心领域。多模态学习可以通过融合不同数据源中的信息

给网络攻击检测系统带来更多的特性,以提高精确度与鲁棒性。多模态学习可以使用多类型数据源,例如网络流量数据,日志文件,系统调用记录和主机状态信息,并将其整合之后,该模型可以多维度综合分析网络环境。比如网络流量数据能够揭示攻击流量基本特性,日志数据能够给出攻击者入侵痕迹以及系统异常运行情况,主机数据能够帮助发现潜在后门程序以及恶意软件活动等。对这些信息进行融合处理使网络攻击特征更明确、更直观,可以显著提高攻击检测精度。深度神经网络(DNN)作为多模态学习的关键技术,特别适用于处理复杂和多维度的输入数据。通过它的多层非线性结构,DNN能够自动地学习数据的高阶特征,然后当遇到复杂攻击模式时会表现出很强的识别能力。在多模态学习的结构中,DNN有能力处理各种不同的数据输入,例如卷积神经网络(CNN)能够处理图像和时间序列的数据,循环神经网络(RNN)在分析时间序列数据方面表现出色,尤其是在捕获网络攻击行为模式方面具有显著优势。

3.4结合迁移学习和联邦学习,实现模型动态升级与扩展

迁移学习(Transfer Learning)和联邦学习(Federated Learning)是现代AI技术中的两个核心方法,它们为解决这个问题提供了有效的途径。二者各有其独特优点,能有效地促进网络攻击检测模型动态升级和拓展,以应对越来越复杂多样的攻击威胁。迁移学习最基本的原理就是把已经在某个任务上学习过的知识转移到其他有关的任务上,这样就可以避免模型从头训练。在网络攻击检测方面,迁移学习可以有效地解决新型攻击数据缺乏的难题。由于新型攻击模式通常缺少海量标注数据,常规监督学习方法对新型模型进行训练可能耗时耗力。并且该检测模型通过迁移学习能够使现有攻击知识向新攻击类型迁移,从而迅速适应网络安全新威胁。比如,该模型能够把识别DDoS攻击行为的特性移植到识别某一类未知攻击行为中去,以降低对新标记数据的依赖性,并减少模型对新攻击行为的适应能力。迁移学习在减少训练成本的同时也加快了新攻击模式识别的速度,并有效地增强了AI模型应对突发性网络威胁时的响应速度。区别于迁移学习,联邦学习注重对数据进行隐私保护以及分布式训练。传统集中式学习模式中,通常需要将数据传输给中心服务器处理,在一定场景下会有隐私泄露危险。联邦学习是通过在本地节点上保存数据、仅传递模型更新、不参与敏感数据交换来实现对数据隐私的保护。对于网络攻击检测系统而言,联邦学习可以支持多个分布式节点(例如不同网络设备,终端或者企业服务器等)联合训练模型,而且不需要把所有的数据都集中在一台服务器中进行解析。该方法既能有效地保护数据隐私又能增强检测模型普适性与适应性。该方法通过联邦学习使每个节点都能学习到本地攻击模式,更新后的模式上传到中央服务器上,由中央服务器总结和优化各节点模式更新,从而构成了更准确,更动态攻击检测系统。该分布式训练方法可以在没有中央服务器经常更新或者再训练的情况下,随时间推移不断地学习并适应各种新型攻击方式。

4 结束语

人工智能技术在提高网络攻击检测的准确性和效率方面展现出巨大潜力。通过应用数据预处理、轻量级深度学习模型、多模态学习、深度神经网络、迁移学习和联邦学习等技术,可以有效应对网络攻击数据的复杂性、高速网络环境下的实时检测挑战、不同攻击手法导致的检测难度增加以及新兴攻击的模型升级难题。

[参考文献]

[1]董洪蒙.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,2024,53(09):78-80.

[2]孙利宏,宋萍.人工智能技术在网络安全防御中的应用实践[J].科技视界,2024,14(22):59-62.

[3]何强.人工智能在计算机网络技术中的应用探究[J].数字技术与应用,2023,41(10):46-48.

[4]张博,刘绚,于宗超,等.基于人工智能的电力系统网络攻击检测研究综述[J].高电压技术,2022,48(11):4413-4426.

[5]李浥璇.基于态势感知的电网CPS网络攻击检测技术研究[D].西安电子科技大学,2021.

作者简介：

朱磊(1996--),男,汉族,山东德州人,本科,助理工程师,主要从事通信专业方面的研究工作。