人工智能在网络入侵检测中的模型改进与识别效率优化

丁睿

北京三星九千认证中心有限公司，北京市朝阳区，100020；

摘要：近年来，网络攻击手段变得日益多样化和复杂化，传统的入侵检测系统已经无法满足需求。人工智能作为一种新的技术手段，与网络入侵检测系统结合具有良好的优势，本文从入侵检测模型、特征选择、集成学习、深度学习模型优化以及自适应学习等方面对人工智能模型进行了研究，并对这些方法的优缺点进行了比较分析。针对当前网络入侵检测系统存在的识别效率低的问题，本文提出了一种基于人工智能模型改进与识别效率优化技术的网络入侵检测方法。该方法利用模型训练与推理加速方法提升算法性能；通过数据并行计算、分布式存储等技术提高系统性能。

关键词：人工智能；网络入侵检测；模型改进；识别效率优化

DOI：10.69979/3060-8767.25.11.064

引言

随着网络安全问题的日益突出，传统的网络安全防护技术（如防火墙、入侵检测系统等）已经无法满足需求，网络安全防范急需引入新的技术手段。人工智能是近年来出现的一种新技术手段，其能够自动处理大规模数据，识别未知的攻击行为，在网络安全防护领域具有巨大潜力。与传统入侵检测技术相比，人工智能模型具有识别效率高、识别速度快等优点，将人工智能模型应用于网络入侵监测系统中能够有效地提升系统性能。本文结合人工智能模型的优点，对入侵检测系统中的特征选择、集成学习、深度学习模型优化等问题进行研究，并提出了一种基于人工智能模型改进与识别效率优化技术的网络入侵检测方法。

1 网络入侵检测面临的主要挑战

随着网络攻击的多样化、复杂化，传统的入侵检测系统已经无法满足需求，需要引入新的技术手段来提高入侵检测的识别效率和准确性。人工智能技术的出现为入侵检测系统带来了新的机遇和挑战。目前，人工智能模型在入侵检测系统中主要存在以下两方面的问题：第一，虽然人工智能技术在入侵检测领域具有良好的应用前景，但是传统机器学习方法（如支持向量机、决策树）无法有效识别未知攻击行为，导致无法有效地应对网络安全威胁。第二，人工智能模型的识别效率较低，不能满足大规模数据快速处理和实时检测的需求。因此，有必要对入侵监测系统进行改进，提高系统的识别效率[1]。

2 人工智能与入侵检测系统结合的优势

与传统的入侵监测技术相比，人工智能在入侵监测系统中的应用优势主要体现在以下两个方面：一是人工智能模型能够有效地识别未知攻击行为，根据其行为模式进行关联分析，可以快速、准确地进行攻击行为分析。二是人工智能模型能够自动学习、自我进化，有效提升系统识别效率。人工智能模型与入侵检测系统结合能够有效提升网络入侵检测系统的性能，其中，深度学习技术在网络入侵检测系统中应用效果最好。将深度学习模型应用于网络入侵检测系统中，通过模型训练和推理加速方法提升算法性能。此外，使用自适应学习方法优化入侵监测系统的模型，能够有效提高系统性能。

3 人工智能模型在网络入侵检测中的应用现状

3.1 经典人工智能模型综述（如 SVM、随机森林、神经网络等）

SVM （Support Vector Machine）是一种二分类问题的机器学习方法，该方法能够识别分类规则，但无法对未知攻击行为进行准确地判断。随机森林算法（Random Forest）是一种基于决策树算法的机器学习模型，该方法能够对未知攻击行为进行准确地判断，但是需要大量的训练样本。神经网络（Neural Network）是一种基于神经网络算法的机器学习模型，该模型可以对输入数据进行准确地分类。以上三种人工智能模型在网络入侵检测中应用较多，但都存在着一定的局限性，在实际应用中还需要对其进行优化[2]。

3.2 现有模型的识别效率与不足分析

目前，针对入侵检测系统的人工智能模型主要有以下几种：一是基于统计分析的机器学习方法，如支持向量机、决策树、逻辑回归等；二是基于深度学习的机器

学习方法，如卷积神经网络（CNN）、循环神经网络（RNN）、长短时记忆网络（LSTM）等；三是基于集成学习的机器学习方法，如朴素贝叶斯、遗传算法、决策树等。针对上述模型的识别效率与不足之处，研究者进行了如下优化：一是训练时间过长，无法满足实际应用需求；二是识别准确率低，难以达到实际应用需求；三是模型规模过大，难以满足实际应用需求。这些问题严重影响了入侵监测系统的识别效率。

3.3 现有研究的优缺点总结

总体来说，现有的入侵检测模型各有优劣，但它们都存在共同的缺点。首先，从分类效率来看，基于机器学习的检测模型要明显优于基于规则的检测模型；其次，从检测精度来看，基于机器学习的检测模型明显优于基于规则的检测模型；再次，从识别效率来看，基于机器学习的检测模型要明显优于基于规则的检测模型；最后，从安全性来看，基于机器学习的检测模型明显优于基于规则的检测模型。以上结论可以总结为：传统机器学习模式下的入侵监测技术在网络安全领域中虽然效率较高、准确性较好，但识别精度不高、不能适应网络安全领域不断变化发展的需求。

4 网络入侵检测模型的改进方法

4.1 特征选择与数据预处理优化

针对入侵检测系统的特征选择与数据预处理优化问题，研究者主要采取以下两种方法：一是基于神经网络的机器学习算法，如随机森林、支持向量机等；二是基于朴素贝叶斯、遗传算法等方法，如遗传算法、粒子群优化算法等。虽然这些方法都能够有效地降低系统误报率，但它们都具有一定的局限性。例如，在使用随机森林算法时，特征选择的质量会对识别精度产生影响，而在使用粒子群优化算法时，粒子群优化算法对特征选择质量也有一定影响。因此，针对上述问题，研究者需要综合考虑特征选择的质量、模型训练和推理加速以及数据并行和分布式存储等多方面因素[3]。

4.2 模型结构优化与算法改进

针对模型结构优化与算法改进问题，研究者主要采取以下几种方法：一是基于神经网络的机器学习算法，如支持向量机、神经网络等；二是基于决策树的机器学习算法，如决策树、随机森林等；三是基于遗传算法的机器学习算法，如遗传算法、粒子群优化算法等；四是基于集成学习的机器学习算法，如朴素贝叶斯、支持向量机等。尽管这些方法能够有效提高入侵检测模型的识别精度，但它们都具有一定的局限性。例如，对于决策树模型来说，传统的决策树算法只能对一些简单的攻击行为进行准确判断，而对于复杂攻击行为，传统的决策树算法无法进行准确判断。

4.3 集成学习与混合模型设计

针对集成学习模型设计问题，研究者主要采取以下几种方法：一是基于不同算法的集成学习模型，如朴素贝叶斯、支持向量机等；二是基于多算法的集成学习模型，如随机森林、决策树等；三是基于多模型的集成学习模型，如混合学习器、层次分类器等。尽管上述方法都能够有效地提高网络入侵监测系统的识别精度，但它们都存在一定的局限性。例如，在使用多模型时，由于模型复杂度高，往往会导致系统识别准确率降低。因此，研究者需要采用适当的算法设计合适的模型来解决上述问题。此外，在设计集成学习模型时，还需要综合考虑不同算法在系统中的权重。

4.4 深度学习模型改进（如 CNN、RNN、Transformer 等）

深度学习模型是当前机器学习领域的研究热点，在许多领域都取得了良好的效果。然而，深度学习模型存在训练时间长、算法复杂度高等问题，无法有效解决入侵检测系统的识别效率问题。针对上述问题，研究者主要采取以下几种方法：一是深度学习模型优化方法，如采用 CNN、RNN、Transformer 等深度学习模型进行入侵检测系统的优化；二是深度学习模型加速方法，如采用 Fast-CNN、Dropgram 等深度学习模型进行入侵检测系统的加速；三是深度学习模型自适应学习方法，如采用反向传播算法对深度学习模型进行学习[4]。

4.5 异常检测与自适应学习机制

异常检测是一种在异常发生后检测异常的方法，异常检测是通过统计分析将大量数据中的正常模式进行提取，根据不同的模式特征判定是否为异常，并将其作为下一步进行学习的依据。传统的学习方式是通过对历史数据进行分析，在当前网络环境下对未来数据进行预测。当出现新的入侵行为时，根据之前训练好的模型和预测结果来判断当前是否发生了入侵行为，如果发生入侵行为则根据检测结果进行后续的学习。然而在实际应用过程中，网络环境会发生变化，传统学习方式下所训练的模型不能适应当前网络环境的变化，因此需要采用自适应学习机制来更新模型。

5 识别效率优化技术

5.1 模型训练与推理加速方法

深度学习模型的训练与推理是整个系统最耗时的环节，因此对整个系统进行加速能够有效提高模型识别效率。然而，对于入侵检测系统来说，由于数据量较小、识别规模较大，因此并不适合采用深度学习模型进行训练与推理加速。针对上述问题，研究者提出了采用轻量级深度学习模型进行加速的方法，如采用 Fast-CNN 模型进行入侵监测系统的加速；采用 Dropgram 模型进行入侵检测系统的加速；采用 ResNet50 模型进行入侵检测系统的加速。上述方法都能够有效地减少系统训练时间，提高系统识别效率。此外，还需要通过理论分析与实验验证来验证加速方法的有效性。

5.2 轻量级模型与参数优化

轻量级模型是指通过参数化方式对模型进行设计，其主要目的是提高模型的识别效率。为了提高模型的识别效率，研究者在设计轻量级模型时，需要考虑以下几个因素：一是模型的结构参数化，即采用固定结构的轻量级模型；二是参数的数量参数化，即采用少量参数便能满足实际应用需求；三是模型的超参数化，即采用少量超参数便能达到较高的识别效率；四是训练方式参数化，即采用有限次迭代训练方式进行训练。除了上述因素外，还需要考虑不同网络环境对轻量级模型识别效率的影响。在实际应用过程中，还需要结合具体网络环境与网络特征进行具体分析。

5.3 数据并行与分布式计算

对于数据量较大的入侵监测系统来说，对其进行并行化处理与分布式计算是一种有效的方法。例如，在使用深度学习模型进行训练时，研究者可以采用并行化计算的方式，即采用分布式计算方式将各个模型进行并行化训练；在使用机器学习模型进行训练时，研究者可以采用分布式计算方式将各个机器学习模型进行并行化训练。此外，由于网络环境的不确定性，对于不同的网络环境，需要采用不同的数据并行与分布式计算方式[5]。

5.4 实时检测与系统部署优化

在实际应用过程中，入侵检测系统往往需要实时检测大量的攻击数据。然而，由于入侵监测系统的识别效率有限，因此对于大规模入侵数据来说，可能需要多次进行检测才能达到较高的识别精度。因此，对于大规模的网络数据来说，可以采用分布式计算方式来提高入侵监测系统的识别效率。例如，研究者可以采用 MPP 方式对入侵监测系统进行部署，从而减少网络中的数据传输量。此外，还可以采用集群方式来实现分布式计算，从而提高系统的识别效率。除此之外，研究者还可以通过对系统进行调度与调度管理来提高系统的识别效率。这些技术都能够有效地提高入侵监测系统的识别效率。

5.5 评估指标与性能对比分析

本文对网络入侵检测模型进行改进，主要从识别率、检测速度两个方面进行对比分析。本文采用的 ID3 和 ID4 作为数据集，采用 5 折交叉验证法作为模型训练的评价指标。在实际网络环境下，本文对改进模型进行了仿真实验，并与原有模型进行了对比分析。其中，训练集的实验数据量为 100 GB，测试集的数据量为 1 GB。实验结果显示，在相同条件下，改进模型与原始模型在识别率、检测速度上无明显差别。本文研究表明，在训练集数据较少时，改进模型的识别性能优于原始模型。

6 结语

本文对人工智能模型的理论基础、算法结构、特征选择、集成学习以及深度学习模型的优化等问题进行了研究。针对当前网络入侵检测系统识别效率低的问题，提出了一种基于人工智能模型改进与识别效率优化技术的网络入侵检测方法。该方法利用人工智能模型的特征选择和集成学习算法对系统进行改进，提升了网络入侵检测系统的性能。同时，为了进一步提高网络入侵检测系统的识别效率，提出了一种基于数据并行计算和分布式存储技术的网络入侵检测方法。实验结果表明，本文提出的方法在保证检测精度的前提下能够有效地提高系统的识别效率。

参考文献

[1]张杨.人工智能时代网络入侵检测与防御技术[J].数字通信世界,2025,(07):71-73.
[2]路博.人工智能赋能下的网络入侵检测精准模型构建[J].中国宽带,2025,21(08):34-36.
[3]许衡.基于人工智能的网络入侵检测系统设计[J].数字技术与应用,2025,43(06):7-9.
[4]王斌.人工智能在网络入侵检测系统中的应用与优化策略[J].中国宽带,2025,21(03):61-63.
[5]张颢新,刘玉洁,王思成.CNN-RNN 算法在网络入侵检测与信息安全保密技术中的应用研究[J].电脑知识与技术,2024,20(33):44-46.