恶意代码检测方法中的机器学习与深度学习应用研究

李一鸣　谢涛　梅东冬
（宁夏理工学院　宁夏石嘴山　753000）

摘　要：机器学习和深度学习技术在恶意代码检测方面的应用研究越来越受关注。这些技术可以通过对大量样本进行训练，自动学习和提取恶意代码特征，从而实现准确和高效的恶意代码检测。机器学习方法包括传统的特征工程和分类器技术，如支持向量机和随机森林，可以应用于恶意代码检测中。深度学习技术则利用深度神经网络进行自动特征抽取和分类，实现更高的检测准确率。此外，还有一些创新技术如增强学习和迁移学习在恶意代码检测中的应用，进一步提高了检测效果。尽管存在一些挑战，但机器学习和深度学习在恶意代码检测领域具有广阔的应用前景。

关键词：检测方法；机器学习；深度学习

恶意代码的不断演变和增多给计算机系统的安全性带来了严重挑战。传统的恶意代码检测方法往往难以应对新型恶意代码的多样性和变种。因此，引入机器学习和深度学习技术成为提升恶意代码检测效果的一个重要方向。

3 机器学习在恶意代码检测中的应用

3.1 机器学习基础概念回顾

在恶意代码检测中，机器学习技术被广泛应用于恶意代码分类、行为分析和异常检测等任务中。首先，监督学习是一种机器学习方法，通过已标记的训练数据集来训练模型，使其能够从输入数据中学习并进行预测。在恶意代码检测中，监督学习常用于建立恶意代码分类模型。其次，无监督学习是一种机器学习方法，通过未标记的数据进行学习，寻找数据中的潜在结构和模式。在恶意代码检测中，无监督学习可以用于发现异常行为或未知的恶意代码。此外，特征工程是指从原始数据中提取并选择有意义的特征，以供机器学习模型使用。在恶意代码检测中，特征工程起着至关重要的作用，可以影响模型的性能和有效性。另外，在机器学习中，模型的评估是衡量模型预测能力的重要步骤。常用的评估指标包括准确率、召回率、F1 值等，通过这些指标可以评估模型的性能优劣。

3.2 传统机器学习算法在恶意代码检测中的应用

传统机器学习算法在恶意代码检测领域扮演着重要的角色，各种算法都被应用于恶意代码检测任务。首先，支持向量机是一种常用的监督学习算法，在恶意代码检测中被广泛应用于恶意代码分类任务。通过在高维空间中找到最佳的超平面来实现数据的分类。其次，决策树是一种基于树结构的分类算法，在恶意代码检测中可以用于可视化恶意代码的分类过程，同时易于理解和解释。在此，随机森林是一种集成学习算法，结合多个决策树来进行分类，能够有效减少过拟合情况，提高模型的泛化能力。此外，朴素贝叶斯分类器是一种基于贝叶斯定理的统计分类器，在恶意代码检测中可以用于文本分类和特征选择。另外，K 近邻算法是一种简单但有效的分类算法，根据样本之间的距离来进行分类，适用于恶意代码检测中的异常检测任务。

4 深度学习在恶意代码检测中的应用

4.1 深度学习基础概念介绍

深度学习是机器学习领域的一个分支，它通过多层神经网络模型来学习和提取数据中的特征，并进行复杂的模式识别和预测任务。这些深度学习基础概念为恶意代码检测提供了强大的工具和技术。深度学习模型通过学习数据的抽象特征，可以有效地处理复杂的恶意代码检测任务，并取得了显著的成果。深度学习是一种基于人工神经网络的机器学习方法，具有多层神经网络结构。深度学习的基本概念，包括神经网络、前向传播、反向传播等重要概念，以帮助理解深度学习在恶意代码检测中的应用。

4.3 深度学习在恶意代码检测中的实际应用案例

在深度学习在恶意代码检测领域有很多实际应用案例，其中一些案例包括：研究者使用深度学习模型如卷积神经网络和长短期记忆网络来检测恶意代码变种。这些模型能够有效地捕获恶意代码的特征和行为模式，帮助检测新的恶意变种。将图像处理技术和深度学习相结合，将恶意代码文件表示为图像形式，然后使用卷积神经网络来进行检测。这种方法可以提高恶意代码检测的准确性和效率。利用生成对抗网络生成逼真的恶意代码样本，用于增强深度学习模型的训练数据集。这样可以提高模型的泛化能力和对新恶意代码的检测能力。此外，将注意力机制引入到深度学习模型中，帮助模型更好地关注恶意代码中关键的特征和行为，从而提高检测性能和准确性。利用深

度学习模型搭建端到端的恶意代码检测系统，实现对恶意代码的自动检测和分类。这种系统可以帮助安全团队快速发现和应对恶意代码威胁。

这些实际应用案例展示了深度学习在恶意代码检测领域的强大潜力和应用前景。随着深度学习技术的不断发展和完善，相信会有更多创新性的方法和系统被引入到恶意代码检测中，提高网络安全防护水平。现有研究已经证明深度学习在恶意代码检测中取得了显著的成果。

5 增强学习与迁移学习在恶意代码检测中的应用

5.1 增强学习原理与应用

增强学习是一种机器学习方法，其目标是通过与环境的交互学习，使智能体能够从经验中学习并逐步改进决策策略，以达到最大化预期累积奖励的目标。在恶意代码检测领域，增强学习可以被用来培训智能体，以从动态和复杂的恶意代码环境中学习并做出有效的检测决策。

增强学习通过智能体与环境交互，采取行动并观察环境的反馈（奖励），以学习最优的行为策略。智能体根据奖励信号来调整自己的行为，以最大化长期奖励的积累。强化学习通常基于马尔可夫决策过程进行建模，包括状态、动作、奖励等要素。主要算法包括 Q-learning、深度 Q 网络、策略梯度等。另外，在恶意代码检测中，增强学习可以用来训练智能体以自动学习和适应不断变化的恶意代码特征和行为。智能体可以通过与环境交互，逐步优化检测策略，提高检测准确性和泛化能力。在增强学习中，存在探索与利用的权衡。智能体需要在探索未知领域和利用已知信息之间取得平衡，以获取更多关于环境的信息并改进策略。此外，设计合适的奖励函数是增强学习成功的关键。在恶意代码检测中，奖励可以根据检测的准确性、效率以及系统对不同类型恶意代码的处理能力来设计。

5.2 迁移学习原理与应用

迁移学习是一种机器学习方法，旨在通过从一个领域（称为源领域）学习的知识来改善在另一个相关但不同的领域（称为目标领域）上的学习性能。在恶意代码检测中，迁移学习可以用来利用已有的知识并将其应用于新的恶意代码检测任务。

迁移学习旨在通过从源领域学习到的特征、知识、模型参数等信息，来改善在目标领域上的学习效果。它可以通过减少针对目标领域的训练样本数量、提高学习效率以及提升模型泛化能力等方面来实现。迁移学习的关键是如何适应从源领域到目标领域的差异。在恶意代码检测中，源领域可以是已有的恶意代码数据，目标领域可以是新收集的恶意代码数据。通过迁移学习，可以将源领域上学到的恶意代码特征和行为模式应用于目标领域，以提高新恶意代码的检测准确性。可以通过多种策略来实现。一种常见的策略是特征迁移，即使用从源领域学到的特征来提取目标领域的恶意代码特征。另一种策略是模型迁移，即利用从源领域学到的模型参数或模型结构来加速目标领域的训练等。在迁移学习中，一个重要的问题是如何处理源领域和目标领域之间的领域转移。这涉及到源领域和目标领域的相似性、数据分布的差异等因素。可以采用领域适应方法，如对抗训练、领域间的实例加权、特征选择等技术，来减小领域差异。此外，迁移学习还可以利用知识蒸馏技术，将源领域上学到的知识和模型鲁棒性进行压缩，然后将其用于目标领域的学习。这将有助于传递源领域的知识和经验，并提升目标领域的恶意代码检测性能。

7 结论与展望

总之，在恶意代码检测领域，深度学习、增强学习和迁移学习等人工智能技术的应用前景广阔。未来的研究可以从多个方面继续探索和改进，以进一步提高恶意代码检测的准确性、效率和适应性。可以为提高恶意代码检测的准确性和效率提供新思路和方法。这对于保护计算机系统和用户信息安全具有重要意义。通过本研究，可以为未来恶意代码检测技术的发展提供有益的参考和指导。

参考文献：

[1]安磊,韩忠华,林硕,尚文利.面向网络入侵检测的GAN-SDAE-RF模型研究[J].计算机工程与应用, 2021(155-164).

[2]王力,曾文,张运良,等.科技前沿识别体系中的机器学习应用问题[J].科技管理研究, 2023, 43(6):27-35.

[3]高琪琪,师智斌,覃月明,et al.基于API序列的可解释恶意代码检测方法[J].计算机工程与设计, 2023, 44(6):1642-1648.

[4]GAO Bo,DONG Zengbo,LI Fei,等.基于深度学习与改进负荷行为关联图的农业用户非侵入式负荷分解方法[J].电工电能新技术, 2024, 43(1):72-84.

[5]马丹,万良,程琪芩,et al.Attention-CNN在恶意代码检测中的应用研究[J].计算机科学与探索, 2021, 15(4):12.DOI:10.3778/j.issn.1673-9418.2004069.

作者简介：姓名：李一鸣，198403 性别：男 民族：汉 籍贯：吉林省长春市

学历：本科 单位：宁夏理工学院 职务：教师

研究方向：计算机应用。

项目来源“项目名称”：宁夏自然科学基金+面向恶意代码检测的在线迁移学习与多源信息融合技术研究+2022AAC03345