

# 人工智能驱动的网络通信安全：威胁检测与防御策略

王芳艳 谭宇冰

广西农业工程职业技术学院，广西崇左，532100；

**摘要：**随着互联网的普及和信息技术的迅猛发展，网络通信安全面临诸多威胁，如数据泄露、恶意攻击和网络诈骗等。人工智能技术在网络安全领域的应用逐渐受到关注，凭借其强大的数据处理和自主学习能力，能够高效识别和应对各种网络威胁。本文探讨了人工智能驱动的网络通信安全威胁检测与防御策略，分析了人工智能技术在网络通信安全中的应用现状及其优势，详细介绍了基于人工智能的威胁检测模型及其性能评估，并构建了智能化防御策略框架的实施步骤和效果分析。研究表明，人工智能技术显著提升了网络通信安全水平，但仍需不断优化以应对新型攻击手段。未来研究应聚焦于提高模型准确性和实时性，探索轻量级算法，并建立动态更新机制，以构建更加稳固的网络环境。

**关键词：**人工智能；网络通信安全；威胁检测；防御策略；机器学习

DOI: 10.69979/3041-0673.25.12.011

## 引言

网络通信安全是现代社会信息基础设施的重要组成部分，其重要性不言而喻。随着互联网的普及和信息技术的迅猛发展，网络通信已成为人们日常生活和工作中不可或缺的一部分。然而，网络通信的开放性和复杂性也使其面临诸多安全威胁，如数据泄露、恶意攻击和网络诈骗等，严重影响了个人隐私、企业利益乃至国家安全。

在此背景下，人工智能技术在网络安全领域的应用逐渐受到广泛关注。人工智能凭借其强大的数据处理能力和自主学习能力，能够高效识别和应对各种网络威胁，显著提升网络安全防护水平。机器学习和深度学习算法的应用，使得系统能够从海量数据中学习正常行为模式，从而及时发现异常和潜在威胁。

尽管人工智能在网络安全中的应用前景广阔，但仍存在诸多挑战和亟待解决的问题。例如，如何提高威胁检测的准确性和实时性，如何应对不断演变的新型攻击手段，以及如何平衡安全防护与系统性能之间的关系。这些问题不仅需要技术层面的深入研究，还需要结合实际应用场景进行综合考量。

基于上述背景，本文旨在探讨人工智能驱动的网络通信安全威胁检测与防御策略。具体研究问题包括：人工智能技术在网络通信安全中的应用现状及其优势，基于人工智能的威胁检测模型及其性能评估，以及构建智能化防御策略框架的实施步骤和效果分析。通过系统的研究和分析，力求为提升网络通信安全水平提供理论支持和实践指导。

## 1 网络通信安全现状与挑战

当前网络通信安全面临多种威胁，主要包括分布式拒绝服务（DDoS）攻击、恶意软件、钓鱼攻击等。DDoS

攻击通过大量无效请求瘫痪目标服务器，严重影响网络服务的可用性。恶意软件则通过感染用户设备，窃取敏感信息或破坏系统功能。钓鱼攻击则利用伪装成合法实体的手段，诱骗用户泄露个人信息。这些威胁类型各有特点，但共同点是都对网络通信安全构成严重威胁。

现有的安全防御措施主要包括防火墙、入侵检测系统（IDS）、防病毒软件等。然而，这些传统防御手段存在明显局限性。防火墙虽能有效阻止外部攻击，但对内部威胁防范不足。IDS 虽能检测已知攻击模式，但对新型或变异攻击识别能力有限。防病毒软件依赖于签名库更新，难以应对零日攻击。此外，随着网络环境的复杂化和攻击手段的多样化，传统防御措施难以全面覆盖所有安全风险。

在此背景下，人工智能技术在网络通信安全领域的应用展现出巨大潜力。人工智能通过机器学习和深度学习算法，能够实现对海量数据的快速分析，从而有效识别异常行为和潜在威胁。例如，基于人工智能的异常检测系统能够实时监控网络流量，及时发现 DDoS 攻击的前兆。智能化的恶意软件检测则能通过行为分析，识别出传统防病毒软件难以捕捉的新型恶意代码。此外，人工智能在钓鱼攻击识别中的应用，能够通过分析邮件内容和发送者行为，准确判断其合法性。

具体而言，人工智能技术在威胁检测与防御方面的优势主要体现在以下几个方面：一是数据处理能力强，能够高效处理大规模网络数据；二是自主学习能力，能够不断更新和优化检测模型；三是泛化能力强，能够应对多种新型攻击手段。这些优势使得人工智能成为提升网络通信安全的重要技术手段。

为更直观展示当前网络通信安全威胁类型的分布情况，图 1 展示了各类威胁的占比情况（见图 1）。通过该图可以看出，DDoS 攻击、恶意软件和钓鱼攻击占据

了主要比例，进一步印证了上述威胁的严重性。



图1：网络安全威胁类型分布图

综上所述，人工智能技术在应对当前网络通信安全威胁方面具有显著优势，能够有效弥补传统防御措施的不足，为构建更加安全的网络环境提供有力支持。

## 2 人工智能技术在网络通信安全中的应用

人工智能技术，作为一种前沿科技，其基本原理涵盖了机器学习、深度学习和自然语言处理等多个领域。机器学习通过构建数学模型，使计算机系统能够从数据中自主学习并做出预测或决策。深度学习则进一步利用多层神经网络，增强模型对复杂数据的处理能力。自然语言处理则专注于使计算机理解和生成人类语言，广泛应用于文本分析和信息提取。

在网络通信安全领域，人工智能技术的应用主要体现在威胁检测、异常行为识别和攻击预测等方面。首先，威胁检测方面，基于机器学习的异常检测系统能够实时分析网络流量，识别出异常模式。例如，通过监督学习算法，系统可以学习正常网络流量的特征，并在检测到偏离正常模式的数据时发出警报。其次，异常行为识别方面，深度学习技术能够对用户行为进行建模，识别出潜在的恶意行为。具体案例中，某企业利用卷积神经网络（CNN）对用户登录行为进行分析，成功识别出多起账户盗用事件。最后，攻击预测方面，自然语言处理技术通过对网络安全事件的文本数据进行挖掘，能够预测未来可能发生的攻击类型和目标。

人工智能技术在提高网络通信安全效率中的优势显著。首先，其强大的数据处理能力能够高效处理海量网络数据，显著提升威胁检测的实时性和准确性。其次，自主学习能力使得安全系统能够不断从新数据中学习，动态更新检测模型，有效应对新型攻击手段。此外，泛化能力强的人工智能模型能够在面对多样化攻击时，依

然保持较高的识别率。

通过上述分析可以看出，人工智能技术在网络通信安全领域的应用不仅提升了威胁检测和防御的效率，还显著增强了系统的自适应能力，为构建更加稳固的网络环境提供了强有力的技术支撑。

## 3 基于人工智能的威胁检测模型

在网络通信安全领域，基于人工智能的威胁检测模型已成为研究热点。其中，基于神经网络的入侵检测系统和基于异常检测的机器学习模型是两种常见的应用方式。

首先，基于神经网络的入侵检测系统（NIDS）利用深度学习技术，通过构建多层神经网络来识别网络流量中的异常行为。其基本原理是，神经网络通过大量正常和异常网络流量的训练数据，学习并提取特征，从而在新的数据流中识别出潜在的威胁。具体而言，卷积神经网络（CNN）和循环神经网络（RNN）在这一领域应用广泛。CNN擅长处理空间特征，适用于静态数据包的分析；而RNN则擅长处理时间序列数据，适用于动态流量分析。然而，此类模型的训练过程复杂，需要大量标注数据，且在面对新型攻击时，模型的泛化能力可能不足。

其次，基于异常检测的机器学习模型通过分析网络流量的统计特征，识别出与正常行为显著偏离的异常模式。常用的算法包括支持向量机（SVM）、孤立森林（Isolation Forest）和聚类算法等。这些模型的优势在于无需大量标注数据，能够有效发现未知威胁。然而，其缺点在于误报率较高，尤其是在网络环境复杂多变的情况下，模型的鲁棒性受到挑战。

在适用场景方面，基于神经网络的入侵检测系统适用于对实时性和准确性要求较高的场景，如金融交易系统和企业内部网络。而基于异常检测的机器学习模型则更适用于数据量庞大且标注困难的场景，如互联网服务提供商和大型数据中心。

模型的训练和验证过程是确保其性能的关键环节。首先，数据预处理是必不可少的步骤，包括数据清洗、特征提取和归一化等。其次，模型训练阶段，需选择合适的算法和超参数，并通过交叉验证等方法优化模型性能。最后，在验证阶段，使用独立的测试集评估模型的准确率、召回率和F1分数等指标，确保其在实际应用中的有效性。

通过上述分析可以看出，基于人工智能的威胁检测模型在提升网络通信安全方面具有显著优势，但也存在一定的局限性。因此，在实际应用中，需根据具体场景和需求，选择合适的模型并进行优化，以实现最佳的威胁检测效果。

## 4 人工智能驱动的防御策略

在网络通信安全领域，构建基于人工智能的防御策略框架是提升威胁检测与防御能力的关键。该框架旨在通过智能化手段，实现对网络威胁的实时监控、精准识别和有效响应。具体实施步骤如下：

首先，数据收集是基础环节。需从网络设备、服务器和终端等多源收集流量数据、日志信息和用户行为数据。数据的质量和多样性直接影响后续模型的训练效果。其次，数据预处理包括数据清洗、去噪和特征提取，确保输入数据的准确性和一致性。

模型训练是核心步骤。选择合适的机器学习或深度学习算法，如卷积神经网络（CNN）或支持向量机（SVM），利用预处理后的数据进行训练。训练过程中，需不断调整超参数，并通过交叉验证优化模型性能，提高其泛化能力。

实时监控是防御策略的关键环节。部署训练好的模型于网络环境中，实时分析流量数据，识别异常行为。监控系统的设计需考虑实时性和准确性，确保在威胁发生时能够迅速响应。

响应机制是防御策略的最终落实。一旦检测到威胁，系统应立即触发预警，并根据威胁等级采取相应的防御措施，如阻断恶意流量、隔离受感染设备等。同时，记录威胁信息和响应结果，用于后续模型的迭代优化。

讨论策略的有效性和可行性，基于人工智能的防御策略在提升威胁检测的准确性和实时性方面具有显著优势。然而，其实施需依赖高质量的数据和高性能的计算资源，且模型的更新和维护需持续投入。因此，在实际应用中，需综合考虑成本、技术和环境因素，确保策略的可行性和持续性。

通过上述步骤，基于人工智能的防御策略框架能够有效提升网络通信安全水平，为构建安全稳定的网络环境提供有力保障。

## 5 案例分析

在网络通信安全领域，人工智能技术的应用已展现出显著成效。以某大型金融机构为例，该机构采用基于深度学习的入侵检测系统（IDS），成功识别并防御了多次复杂的网络攻击。该系统利用卷积神经网络（CNN）对网络流量数据进行实时分析，通过学习正常流量模式，有效识别异常行为。实际应用中，该系统能够在毫秒级时间内检测到潜在威胁，并自动触发防御机制，显著提升了网络安全性。

然而，该案例亦暴露出一些问题。首先，数据质量对模型性能影响较大，部分低质量数据导致误报率较高。其次，模型训练需大量计算资源，成本较高。此外，面对新型攻击手段，模型的适应性有待提升。

针对上述问题，提出以下改进建议：首先，加强数

据预处理环节，采用更精细的数据清洗和特征提取技术，提高数据质量。其次，优化模型结构，探索轻量级神经网络，降低计算资源需求。最后，建立动态更新机制，定期更新训练数据，提升模型对新威胁的识别能力。

另一案例为某互联网公司部署的基于机器学习的恶意流量检测系统。该系统采用支持向量机（SVM）算法，通过对流量特征的深度挖掘，有效识别恶意流量。实际运行中，系统显著降低了恶意攻击的成功率。但同样存在误报率高、模型更新滞后等问题。建议引入自适应学习机制，实时调整模型参数，增强其对动态威胁的应对能力。

通过上述案例分析，可见人工智能技术在网络通信安全中的应用虽取得一定成效，但仍需不断优化和改进，以应对日益复杂的网络安全挑战。

## 6 结论与展望

人工智能技术在网络通信安全中的应用，显著提升了威胁检测与防御能力。其强大的数据处理和自主学习能力，有效应对了多样化攻击手段，弥补了传统防御措施的不足。未来研究应聚焦于提高模型准确性和实时性，探索轻量级算法以降低资源消耗，并建立动态更新机制以适应新型威胁。同时，跨领域融合与标准化建设亦为重要方向，以构建更加智能、高效的网络安全防护体系。

## 参考文献

- [1] 张兴富, 李燕, 张金帅, 等. 端边云协同的分布式人工智能模型训练与推理优化[J/OL]. 现代应用物理, 1-15[2025-06-17]. <http://kns.cnki.net/kcms/detail/61.1491.04.20250616.1817.010.html>.
- [2] 裴雅, 李亚珂. 数据加密技术在计算机网络通信安全中的应用探究[J]. 信息记录材料, 2025, 26(04): 87-89. DOI: 10.16009/j.cnki.cn13-1295/tq.2025.04.026.
- [3] 姚驰. 基于人工智能的网络安全威胁检测与防御策略研究[J]. 中国宽带, 2025, 21(05): 52-54. DOI: 10.20167/j.cnki.ISSN1673-7911.2025.05.18.
- [4] 牟杨城, 陈爱网, 陈桂茸, 等. 基于数据投毒攻击的联邦学习安全防御策略[J/OL]. 系统工程与电子技术, 1-14[2025-06-17]. <http://kns.cnki.net/kcms/detail/11.2422.TN.20250523.1048.051.html>.
- [5] 周知勤, 刘凤麟. 基于 Python 的生态学数据分析与机器学习实验设计[J/OL]. 实验科学与技术, 1-7[2025-06-17]. <http://kns.cnki.net/kcms/detail/51.1653.N.20250609.1843.003.html>.

作者简介：王芳艳（1995.1-）女，汉，广西桂林，本科，研究方向为网络安全。