基于深度学习的网络攻击检测与防御策略创新

冯征辉　叶　涵
河北方维网络技术有限公司　河北　石家庄　050000

摘　要：在信息技术飞速发展的今天，网络攻击的手段也越来越多样化、复杂化，给网络安全带来了严重的威胁。本研究旨在通过深度学习探索网络攻击检测及防御策略的创新之处，以期在网络安全领域中提供一种新思路、新途径。首先对网络攻击检测研究的意义与挑战及深度学习在这一领域中的应用进行分析。接下来，文章深入阐述了一个网络攻击检测模型，该模型基于卷积神经网络、双向长短时记忆网络、注意力机制，并整合了多种深度学习技术。并以此为基础进一步讨论基于深度强化学习，自编码器以及Petri网建模等网络攻击防御策略的创新。这些研究结果对于提高网络攻击检测准确性与效率、建设智能网络安全防护体系等方面提供了一种新技术手段与新思路。

关键词：深度学习；网络攻击检测；网络防御策略；卷积神经网络；智能安全防护

引言

信息技术的快速发展在大大促进社会进步的同时，随之而来的网络安全问题却越来越突出。网络攻击手段日益翻新与复杂化给原有网络安全防护体系带来了严峻的挑战。在这种情况下，深度学习技术凭借强大的数据处理能力以及模式识别能力为网络攻击检测及防御提供一种全新的解决思路。本论文围绕基于深度学习创新网络攻击检测和防御策略进行研究，目的在于探索出一条更有效，更准确的网络安全防护新途径。

1 基于深度学习的网络攻击检测技术概述

1.1 网络攻击检测的重要性与挑战

网络攻击检测通过对网络流量和系统日志进行数据分析来确定可能存在的攻击行为并据此采取防御措施。该流程对保持网络系统安全具有重要意义。[1]随着网络技术的迅猛发展，网络攻击手段不断进化并呈现多样化和隐蔽化特征。传统基于特征匹配检测方法面对新的攻击通常无能为力，很难进行有效的识别。另外，网络攻击通常存在跨平台和跨协议等问题，这就增加了检测的复杂性。所以如何提高测试的准确性，实时性以及适应性是目前网络攻击测试所面临的重大挑战。

网络攻击检测不仅具有能及时发现并防御攻击、降低潜在损失等重要意义，而且具有对网络安全态势感知预警功能。对网络流量进行连续的监测与分析，能够及时发现网络中的异常情况，从而为网络的安全管理提供决策支持。与此同时，网络攻击检测在网络安全防御体系中占据着举足轻重的地位，它和防火墙，入侵防御系统及其他安全措施互相配合构成了一个多层次防御体系。

网络攻击的检测同样面临许多挑战。一是网络攻击手段在不断地进化，增加了探测的难度。攻击者使用多种技术手段例如加密通信和僵尸网络以避免被发现。二是复杂的网络环境也对检测提出挑战。网络流量具有多样性，动态性及海量性等特点，导致检测系统所需处理与分析数据量激增。另外，误报、漏报等问题都是网络攻击检测中亟待解决的难题。误报给用户带来不必要的资源浪费与麻烦，漏报有可能使得攻击行为无法进行并产生严重的后果。

1.2 深度学习在网络攻击检测中的应用

深度学习技术应用于网络攻击检测领域，主要表现为它具有较强的数据处理能力以及特征提取能力。[2]首先，深度学习可以高效地对高维数据进行处理。网络流量数据一般都具有高维度特征，常规机器学习方法处理此类数据常常遭遇维度灾难。深度学习模型，例如卷积神经网络（CNN）和循环神经网络（RNN），具有通过多级非线性转换来自动抽取数据高级特征的能力，从而在高维空间内实现高效的模式识别。

其次，深度学习可以捕获数据中复杂模式。网络攻击行为通常具有模式复杂、动态变化等特征，而传统基于规则方法难以对其进行精确辨识。深度学习模型尤其是自适应学习能力强的神经网络可以对这些复杂模式进行数据学习和有效泛化检测。

再者，深度学习可以增强检测实时性。网络攻击检测要求对网络流量进行实时分析并迅速发现潜在攻击行为。深度学习模型，特别是像MobileNet和ShuffleNet这样的轻量级网络架构，能在维持较高的检测准确性的同时，也能实现快速的数据处理和响应能力。

最后，深度学习可以适应新型攻击手段。在网络攻击手段不断发展变化的情况下，常规检测方法通常需要对规则及特征库进行更新。并且深度学习模型可以通过

不断地学习新数据来自动地适应新攻击模式以降低对人工干预依赖程度。

1.3 基于深度学习的网络攻击检测模型概述

以深度学习为基础的网络攻击侦测模型主要可以被划分为几个主要类别，其中之一是基于卷积神经网络（CNN）的模型。CNN作为深度学习的常见模型之一，利用卷积层与池化层对数据进行空间特征提取。网络攻击检测时，可利用CNN对网络流量数据进行特征提取，例如包大小和包间隔来确定攻击行为。以LeCun等为例，LeNet-5模型是典型的CNN结构之一，在图像识别领域中已经有了令人瞩目的成就。网络攻击检测时，可参考LeNet-5结构设计适用于网络流量数据检测的CNN模型。

这是一个基于循环神经网络（RNN）构建的模型。RNN作为一个能对序列数据进行处理的神经网络，采用循环连接的方式捕获数据中的时间依赖性信息。网络攻击检测时，可利用RNN对网络流量时间序列特征进行分析，例如流量波动情况，异常峰值情况。以LSTM（长短期记忆网络）和GRU（门控循环单元）为例，这两种RNN的变种都能高效地处理传统RNN中的梯度消失问题，并在处理序列数据时展现出卓越的性能。

从注意力机制出发，建立一个模型。注意力机制就是能使模型集中在数据重要组成部分上的一种技术。对于网络攻击检测，注意力机制有助于模型发现流量数据的关键特征以提高检测精度。如Bahdanau等以注意力机制为基础建立的序列对序列模型通过计算输入序列与输出序列间的权重来对输入序列进行高效的编码与解码。

2 基于深度学习的网络攻击检测模型研究

2.1 基于卷积神经网络的网络攻击检测模型

卷积神经网络（CNN）作为一种先进的深度学习模型，在图像和语音识别等多个领域有着广泛的应用。在网络攻击检测方面，CNN能有效提取网络流量数据的特征并实现攻击行为识别。CNN模型采用卷积层、池化层以及全连接层的结构实现了对数据局部特征与全局特征的自动学习，从而提升了检测精度。[3]

在建立基于CNN网络攻击检测模型的过程中，必须先对网络流量数据做预处理，其中包括数据清洗和归一化操作。接着将预处理过的数据送入CNN模型进行训练并对数据进行模式学习。CNN模型中关键是卷积核设计问题，选取适当的卷积核尺寸与步长可在不同规模下进行特征提取。另外，通过调节卷积层个数与深度来增强模型表达能力。

2.2 基于双向长短时记忆网络的网络攻击检测模型

长短时记忆网络（LSTM）是一种特殊的循环神经网络（RNN），能够解决传统RNN在处理长序列数据时的梯度消失问题。LSTM引入了门控机制对时间序列数据的长期依赖关系进行了有效捕捉。在网络攻击检测方面，LSTM能够对网络流量数据进行时间特性处理，提高了检测精度。

双向长短时记忆网络（Bi-LSTM）作为LSTM的一种扩展形式，能够在每一个时间步骤中同时处理过去和未来的数据，从而更全面地捕捉数据的时间属性。构造基于Bi-LSTM网络攻击检测模型时需先对网络流量数据进行序列化以形成时间序列。接着，序列化后的数据被送入Bi-LSTM模型，并通过对数据进行时序模式训练和学习。

Bi-LSTM模型最关键的优点是它处理时间序列数据。其能够有效捕获网络流量数据的动态变化与变化趋势，并对攻击行为时序特征进行识别。另外Bi-LSTM模型泛化能力较好，能够适应各种网络环境及攻击类型。但是Bi-LSTM模型对于大规模数据处理具有很高的计算复杂度，因此需要对模型结构以及训练策略进行优化才能提高探测的效率。

2.3 基于注意力机制的网络攻击检测模型

注意力机制在深度学习领域起着至关重要的作用，它的核心思想就是通过模型对输入数据的关键部分进行自适应注意，以增强模型识别能力。在网络攻击检测方面，注意力机制模型有助于对网络流量异常特征进行关注，从而有效地增强了检测精度。[4]比如，该模型通过构造注意力层可以确定网络流量的关键包，其中可能含有攻击行为的关键信息。更进一步地说，注意力机制有可能与卷积神经网络或长短时记忆网络等不同的深度学习模型进行融合，从而构建一个更加复杂的网络架构，以更好地应对不断变化的网络攻击模式。

2.4 融合多种深度学习技术的网络攻击检测模型

在深度学习技术蓬勃发展的今天，单一模型通常很难处理复杂网络攻击探测任务。所以，将各种深度学习技术进行整合就成了一种有效提升检测性能的方法。例如，通过整合卷积神经网络在局部特征提取方面的能力和长短时记忆网络在时间序列建模方面的专长，我们能够构建一个能够同时处理空间和时间信息的深度学习模型。另外，引入注意力机制能进一步提高模型捕获关键信息的能力。通过该多技术融合，能够构造更有力的网络攻击检测模型来有效地应对各类网络攻击行为。

3 基于深度学习的网络攻击防御策略创新

3.1 基于深度强化学习的智能网络安全防护

深度强化学习是深度学习的重要分支之一，将强化学习和深度学习结合起来可以有效解决网络安全动态决

策难题。[5]在智能网络安全保护方面，采用基于深度强化学习的方法可以实时识别和应对网络攻击行为，从而提升网络安全防护的自动化和智能化程度。基于深度强化学习的智能网络安全防护策略包括如下内容：采用深度学习技术提取网络流量特征并加以分析，以达到区分正常流量与异常流量；利用强化学习算法训练智能体面对网络攻击的最优响应策略以增强识别与防御能力；与多智能体系统相结合，实现了多智能体协同防御，增强了网络安全防护总体效果；采用深度强化学习算法在线优化网络安全策略，达到快速适应网络环境变化。

3.2 基于深度学习的分层网络攻击识别与未知攻击检测

分层网络攻击识别就是把网络攻击检测任务拆分成若干层，每一层负责对各种攻击行为进行检测。采用分层方法提高了检测精度与效率。与此同时，对未知攻击进行检测是当前网络安全领域中一个重要的研究领域。基于深度学习分层的网络攻击识别和未知攻击检测策略包括如下内容：采用深度学习技术多层次提取网络流量特征，以达到识别不同攻击行为类型的目的；利用自编码器这种无监督学习方法建立正常流量模型以达到未知攻击检测的目的；将有监督学习与无监督学习相结合，增强了已知攻击与未知攻击检测能力；将深度学习模型应用于网络攻击行为分类与聚类中，以达到对攻击行为深入剖析与理解的目的。

3.3 基于Petri网建模的工业控制系统网络攻击检测方法

工业控制系统是国家关键基础设施的一个重要组成部分，其安全性直接影响到国家的安全和社会的稳定。但是工业控制系统经常会受到复杂网络攻击的威胁。利用Petri网建模进行网络攻击检测的方法，可以对工业控制系统网络攻击行为进行有效分析与辨识。

采用Petri网进行建模的工业控制系统网络攻击检测手段主要涵盖了以下几个关键领域：通过Petri网对工业控制系统的网络架构和行为模式进行建模，从而实现系统内部状态的可视化展示；通过对Petri网模型进行分析，辨识出系统潜在的安全漏洞以及攻击路径；结合深度学习技术训练并优化Petri网模型以提高网络攻击检测精度与实时性；采用Petri网模型形式化地描述网络攻击行为并进行推理，以达到快速识别攻击行为并做出反应的目的。

4 结束语

文章对基于深度学习创新网络攻击检测和防御策略进行深入探究，目的是迎接日益严重的网络安全挑战。运用对比分析、逻辑推理等方法揭示深度学习技术应用于网络攻击检测、防御等领域的诸多影响要素，反映学术论文复杂分析及批判性思考能力。研究结论显示：基于深度学习进行网络攻击检测和防御策略创新可以有效提升网络安全防护能力和应对复杂多样网络攻击的能力。但深度学习模型在泛化能力，可解释性以及实时性等方面还有待深入研究与完善。

参考文献

[1]马晓欢,李祉岐,王悦振,等.网络攻击和网络攻击事件判定研究[J].信息技术与标准化,2024(4):28-34.

[2]李永娜,张锐.基于机器学习的网络攻击检测与防御方法研究[J].信息与电脑,2024(1):177-179.

[3]黄燕,李金灿,杨霞琴,等.基于深度自编码器的智能电网窃电网络攻击异常检测[J].电子技术应用,2024(2):76-82.

[4]张雷明.基于大数据分析的网络攻击行为预测与防御策略研究[J].信息记录材料,2024(4):40-42.

[5]张雅茹.一种基于半监督学习算法的网络攻击检测系统[J].辽东学院学报：自然科学版,2024(1):47-53.