王治军, 关卿. 人工智能技术在计算机网络防御中的应用研究[J]. 智能计算机与应用,2026,16(5):161-167. DOI:10.20169/j.issn.2095-2163.24082501

人工智能技术在计算机网络防御中的应用研究

王治军[1], 关 卿[2]
(1 武警河南总队, 郑州 450004; 2 中国人民解放军 63893 部队, 河南 洛阳 471003)

摘 要: 随着信息技术的迅猛发展,计算机网络已成为现代社会不可或缺的一部分。然而,网络攻击和恶意行为也随之增加,对网络安全构成了严重威胁。传统的防御手段已难以应对当前复杂多变的网络威胁,因此,探索新的防御技术显得尤为重要。人工智能技术因其强大的数据处理和模式识别能力,在计算机网络防御中展现出巨大潜力。本文旨在探讨人工智能技术在计算机网络防御中的应用。通过理论分析、模型构建、仿真实验以及实验结果评估,验证不同模型在检测网络攻击中的性能,选用支持向量机(SVM)、卷积神经网络(CNN)以及结合循环神经网络(RNN)和生成对抗网络(GAN)的复合模型,并在 KDD Cup 99 和 CICIDS2017 两个公开数据集上进行实验。实验结果表明,RNN+GAN 模型在计算机网络防御中展现出强大的性能,能够有效提高网络攻击的识别准确率和可靠性,是未来网络防御领域研究和应用的方向。

关键词: 人工智能; 计算机网络防御; 循环神经网络; 生成对抗网络; 支持向量机; 卷积神经网络
中图分类号: TP393 **文献标志码**: A **文章编号**: 2095-2163(2026)05-0161-07

Research on the application of artificial intelligence technology in computer network defence

WANG Zhijun[1], GUAN Qing[2]
(1 Henan Armed Police Corps, Zhengzhou 450004, China; 2 Unit 63893, Chinese People's Liberation Army, Luoyang 471003, Henan, China)

Abstract: With the rapid development of information technology, computer networks have become an indispensable part of modern society. However, network attacks and malicious behaviours have also increased, posing a serious threat to network security. Traditional means of defence have been difficult to meet the current complex and changing network threats, so it is particularly important to explore new defence technologies. Artificial intelligence technology shows great potential in computer network defence due to its powerful data processing and pattern recognition capabilities. The purpose of this paper is to explore the application of artificial intelligence technology in computer network defence. Through theoretical analysis, model construction, simulation experiments and evaluation of experimental results, we verify the performance of different models in detecting network attacks, and select the Support Vector Machines (SVM), Convolutional Neural Networks (CNN), and the composite model combining Recurrent Neural Networks (RNN) and Generative Adversarial Networks (GAN). Experiments were conducted on two public datasets, KDD Cup 99 and CICIDS 2017. The RNN+GAN model shows powerful performance in computer network defence, which can effectively improve the identification accuracy and reliability of network attacks, and it is the future research and application direction in the field of network defence.

Key words: artificial intelligence; computer network defence; recurrent neural network; generative adversarial network; support vector machine; convolutional neural network

0 引 言

人工智能技术,特别是支持向量机(SVM)[1]、卷积神经网络(CNN)[2]、循环神经网络(RNN)和生成对抗网络(GAN)[3],因其强大的数据处理与模式识别能力,在计算机网络防御领域展现出巨大潜力[4-8]。本文旨在探讨这些先进的人工智能技术在网络安全中的应用原理、模型构建、算法实现及实验评估,以期为计算机网络防御提供新的思路和方法。通过深入研究 SVM、CNN 以及 RNN 与 GAN 结合的

作者简介: 王治军(1978—),男,硕士,高级工程师。主要研究方向:网络安全。Email:357409831@qq.com;关 卿(1980—),女,硕士,工程师。主要研究方向:电子对抗训练。

收稿日期: 2024-08-25

创新模型,期望能够提升网络防御的智能化水平,有效应对各类网络威胁,保障网络空间的安全稳定。

1 相关理论分析

1.1 支持向量机原理及在网络安全中的适用性

支持向量机是一种基于监督学习的算法,其核心思想是通过寻找一个超平面来最大化不同类别样本间的间隔,从而实现高效分类[1]。在网络安全领域,SVM 可用于识别和分类网络流量中的正常行为和异常行为。由于其出色的分类性能和泛化能力,SVM 在检测网络攻击、恶意软件通信等方面具有广阔的应用前景[9-10]。

1.2 卷积神经网络原理及在网络安全中的优势

卷积神经网络是一种深度学习模型,特别适用于处理图像数据[11]。其通过卷积层、池化层等结构自动提取特征,并用于分类或回归任务。在网络安全领域中,CNN 可应用于网络流量的特征提取和分类。与传统的机器学习算法相比,CNN 能够自动学习并提取高层次的特征,从而更精准地识别复杂的网络攻击模式[12]。这一优势使得 CNN 在网络安全防御中具备巨大的潜力。

1.3 生成对抗网络原理及其在网络安全中的潜力

生成对抗网络由生成器和判别器两部分组成,通过对抗训练生成全新的数据样本[3]。在网络安全领域,GAN 可用于生成模拟的攻击流量,以此增强防御系统的鲁棒性。通过训练判别器区分真实的攻击流量与生成器生成的模拟流量,显著提升防御系统对未知攻击的检测能力。GAN 还可生成多样化的攻击样本,帮助研究人员更好地理解和应对新型网络攻击,在网络安全防御中具备巨大的研究潜力和应用价值[13]。

2 模型构建与算法实现

2.1 SVM 模型在计算机网络防御中的构建与实现

在计算机网络防御中,SVM 模型主要用于分类与识别网络流量中的正常行为和异常行为[14]。为了实现这一目标,首先需要构建合适的特征向量来表示网络流量。特征向量可以包括流量的统计特性、时间特性以及协议特性等。在 SVM 模型的构建过程中,使用核函数来将输入的特征向量映射到高维空间,并在这个空间中寻找一个最优的超平面来分隔正常流量和异常流量。常用的核函数包括线性核、多项式核和高斯核等。

为了实现 SVM 模型,可以使用如下的数学公式来表示:

$$\min_{w,b} \frac{1}{2} \| \boldsymbol{w} \|^2 + C \sum_i \xi^{(i)}$$
$$\text{s.t.} \begin{cases} y^{(i)}(\boldsymbol{w}^{\mathrm{T}} \boldsymbol{x}^{(i)} + b) \geqslant 1 - \xi^{(i)} \\ \xi^{(i)} \geqslant 0 \end{cases}, \forall i = 1,2,\cdots,N \tag{1}$$

其中,$\boldsymbol{w}$ 是权重向量;b 是偏置项;$\boldsymbol{x}^{(i)}$ 是特征向量;$y^{(i)}$ 是样本标签(正常或异常);$\xi^{(i)}$ 是松弛变量,用于处理线性不可分的情况;C 是正则化参数,用于控制模型的复杂度。

2.2 CNN 模型在计算机网络防御中的构建与实现

CNN 模型在计算机网络防御中主要用于特征提取和分类[15]。为了构建 CNN 模型,需要确定输入层、卷积层、池化层、全连接层以及输出层的结构和参数。在 CNN 模型中,卷积层负责提取网络流量的局部特征,池化层用于降低特征维度并增强模型的鲁棒性,全连接层则用于将提取的特征映射到分类结果上。

为了实现 CNN 模型,可以使用如下公式来表示卷积层和池化层的操作:

$$f_{\text{conv}}(\boldsymbol{x}) = \sigma(\boldsymbol{w}_{\text{conv}}) \cdot \boldsymbol{x} + b_{\text{conv}} \tag{2}$$
$$f_{\text{pool}}(\boldsymbol{x}) = \text{pool}(f_{\text{conv}}(\boldsymbol{x})) \tag{3}$$

其中,$f_{\text{conv}}(\boldsymbol{x})$ 表示卷积层的输出;$\sigma(\cdot)$ 表示激活函数(如 ReLU);$\boldsymbol{w}_{\text{conv}}$ 和 b_{conv} 分别表示卷积层的权重和偏置;$f_{\text{pool}}(x)$ 表示池化层的输出;pool(·)表示池化操作(如最大池化或平均池化)。

2.3 RNN+GAN 模型在计算机网络防御中的创新应用

RNN+GAN 模型结合了循环神经网络和生成对抗网络的优势,用于生成和检测复杂的网络攻击模式。在 RNN+GAN 模型中,RNN 用于处理时间序列数据,能够捕捉网络流量中的时间依赖性[16],而 GAN 则用于生成模拟的攻击流量,增强防御系统的鲁棒性[17]。

为了实现 RNN+GAN 模型,可以使用如下公式来表示 RNN 和 GAN 的结合:

$$h_t = \sigma(\boldsymbol{W}_{\text{RNN}} \cdot [h_{t-1}, x_t] + b_{\text{RNN}}) \tag{4}$$
$$G(z) = \tanh(\boldsymbol{W}_G \cdot z + b_G) \tag{5}$$
$$D(x) = \sigma(\boldsymbol{W}_D \cdot x + b_D) \tag{6}$$

其中,h_t 表示 RNN 在时刻 t 的隐藏状态;σ 表示激活函数;$\boldsymbol{W}_{\text{RNN}}$ 和 b_{RNN} 分别表示 RNN 的权重和偏置;$G(z)$ 表示生成器的输出,用于生成模拟的攻击流量;$D(x)$ 表示判别器的输出,用于区分真实的网络流量和生成的模拟流量;$\boldsymbol{W}_G$、b_G、$\boldsymbol{W}_D$ 和 b_D 分别表示生成器和判别器的权重和偏置。通过训练

RNN+GAN 模型，可以提高计算机网络防御系统对未知攻击的检测能力。

3　模拟仿真实验设置与步骤

3.1　实验设置

3.1.1　数据集

为了验证人工智能技术在计算机网络防御中的有效性，本实验选择了两个公开的数据集：KDD Cup 99 数据集[18]和 CICIDS2017 数据集[19]。KDD Cup 99 数据集是一个经典的网络入侵检测数据集，包含了大量的正常和异常网络流量样本。CICIDS2017 数据集则是一个较新的数据集，包含了更多种类的现代网络攻击，如 DDoS 攻击、Botnet 攻击等。这两个数据集能够全面评估模型在不同网络环境下的防御能力，两个数据集的特性比较见表 1。

表 1　KDD Cup 99 与 CICIDS2017 数据集特性对比分析

Table 1　Comparison and analysis of characteristics between KDD Cup 99 and CICIDS2017 datasets

数据集	样本总数	正常样本数	异常样本数	攻击类型数	特征维度	缺失值比例
KDD Cup 99	494 021	97 278	396 743	22	41	0.010
CICIDS2017	2 274 767	1 673 570	601 197	14	80	0.005

从表 1 中可以看出，两个数据集在样本总数、正常样本数、异常样本数、攻击类型数、特征维度以及缺失值比例等方面均存在差异。KDD Cup 99 数据集包含更多的攻击类型，但特征维度相对较低，且存在一定的缺失值比例。而 CICIDS2017 数据集则包含更多的样本和更高的特征维度，缺失值比例较低。这些差异将对后续的模型训练和性能评估产生重要影响。

3.1.2　数据的预处理

预处理流程涉及多个关键步骤，旨在增强数据集的可用性和模型训练的效能。首先实施数据清洗，通过移除重复记录并妥善处理缺失值，确保数据集的完整性和准确性，为后续分析奠定坚实基础。其次进行特征选择，依据网络流量的内在特性，精心挑选出诸如流量大小、持续时间、协议类型及端口号等关键特征，以构建高效表征网络行为的特征向量。接着采用数据标准化方法，将所有特征值统一缩放至相同量级，有效规避了特定特征在模型训练过程中可能产生的支配效应，确保了模型学习的均衡性。最后执行标签编码操作，将类别型标签转换为数值形式，此举旨在提升模型处理效率，便于机器学习算法直接应用于分类任务中。

3.1.3　实验环境

实验环境包括硬件和软件两部分。硬件方面，采用高性能服务器，配备多核 CPU 和高速内存，以确保模型训练的高效性。软件方面，选择 Python 作为编程语言，利用 TensorFlow[20]等深度学习框架来搭建和训练模型。同时，安装必要的库和工具，如 Pandas 用于数据处理，Scikit-learn 用于传统机器学习算法的实现，NumPy 用于数值计算等。

在实验环境配置阶段，为提升实验的稳健性与可重复性，注重以下几方面的优化措施：一是实施严格的版本控制策略，以确保所有依赖的软件库与工具均维持版本一致性，从而规避潜在的版本冲突问题；二是充分利用多核 CPU 的并行处理优势，通过并行计算技术显著提升模型训练与数据处理的执行效率；三是实施详尽的日志记录机制，对实验流程中的关键环节与关键成果进行系统性文档化，为后续的数据分析与实验复现提供坚实支撑。

3.2　实验步骤

本研究在仿真实验部分，遵循科学严谨的研究方法，对支持向量机（SVM）、卷积神经网络（CNN）以及结合了循环神经网络（RNN）和生成对抗网络（GAN）的复合模型进行了全面的训练和测试。

在模型训练阶段，本研究使用了预处理后的 KDD Cup 99 和 CICIDS2017 数据集。为了避免过拟合，采用了 5 折交叉验证的方法。同时，使用了 Adam 优化器[21]来更新模型权重，并设定训练的目标是最小化分类错误率。对于 SVM，使用了径向基函数（RBF）作为核函数[22]，并通过网格搜索来确定最佳的惩罚参数 C 和核函数参数 γ。实验步骤如下：

步骤 1　加载并预处理了 KDD Cup 99 和 CICIDS2017 数据集；

步骤 2　定义模型训练函数；

步骤 3　5 折交叉验证；

步骤 4　根据模型类型配置优化器和损失函数（这里简化为统一设置）；

步骤 5　编译模型；

步骤 6　训练模型，使用 RBF 核；

步骤 7　测试模型性能，使用独立的测试集，测试集是从原始数据集中随机抽取的一部分样本，用于模拟实际网络环境中的未知数据。将测试集输入

到训练好的模型中,得到预测结果,并与实际标签进行对比,计算出各种性能指标。

4 实验评估指标及其结果分析

4.1 实验评估指标

4.1.1 准确率(Accuracy)

准确率是衡量分类模型性能的关键指标,其反映了模型正确分类的样本数占总样本数的比例,计算方法如下:

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN} \tag{7}$$

式中:TP 表示模型将正例正确地预测为正例的数量,FP 表示模型将负例错误地预测为正例的数量,FN 表示模型将正例错误地预测为负例的数量,TN 表示模型将负例正确地预测为负例的数量。

在计算机网络防御的上下文中,准确率高意味着模型能够更准确地识别出网络攻击,这对于提高防御系统的有效性至关重要。

4.1.2 精确率(Precision)

精确率是衡量分类模型性能的另一个重要指标,其反映了模型预测为正类的样本中,真正为正类的样本所占的比例,计算方法如下:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{8}$$

式中:TP 表示模型将正例正确地预测为正例的数量,FP 表示模型将负例错误地预测为正例的数量,

在计算机网络防御的场景中,精确率高意味着模型能够更准确地识别出真正的网络攻击,减少误报的情况,提高防御系统的效率和可靠性。

4.1.3 召回率(Recall)

召回率是衡量分类模型性能的另一个关键指标,其反映了模型能够识别出的真正正类样本占所有实际正类样本的比例,计算方法如下:

$$\text{Recall} = \frac{TP}{TP + FN} \tag{9}$$

式中:TP 表示模型将正例正确地预测为正例的数量,FN 表示模型将正例错误地预测为负例的数量。

在计算机网络防御的场景下,召回率高意味着模型能够更全面地识别出网络攻击,减少漏报的情况,这对于确保网络安全至关重要。

4.1.4 $F1$ 分数($F1$-Score)

$F1$ 分数是衡量分类模型性能的综合性指标,其综合考虑了精确率和召回率,是两者的调和平均数,计算方法如下:

$$F1 = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{10}$$

式中:Precision 表示精确率,Recall 表示召回率。

在计算机网络防御的实践中,$F1$ 分数的高低直接反映了模型在识别网络攻击时的整体性能。一个高 $F1$ 分数的模型意味着其在减少误报和漏报方面都有出色的表现。

4.2 基于 SVM、CNN 和 RNN+GAN 模型的初步实验

针对 KDD Cup 99 和 CICIDS2017 数据集,采用基于 SVM 模型的网络防御方法,基于 CNN 模型的网络防御方法[23]和基于 RNN+GAN 模型的网络防御方法,分别从准确率、召回率、$F1$ 分数和 ROC AUC 四个性能指标评估两种方法,实验结果如图 1—3 所示。

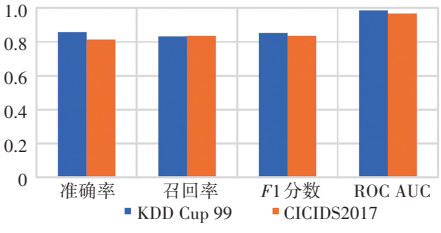


图 1 SVM 模型测试初步分析

Fig. 1 Preliminary analysis of SVM model testing

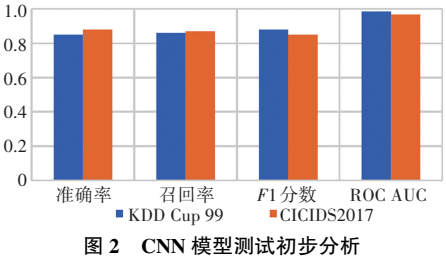


图 2 CNN 模型测试初步分析

Fig. 2 Preliminary analysis of CNN model testing

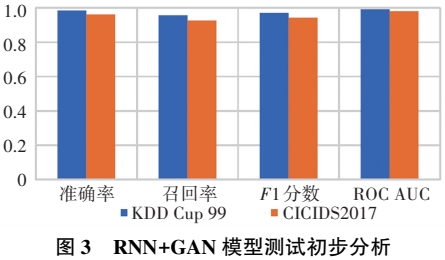


图 3 RNN+GAN 模型测试初步分析

Fig. 3 Preliminary analysis of RNN+GAN model testing

实验结果分析:

(1)如图 1—3 所示,SVM 模型在两个数据集上都取得了不错的性能指标,但相较于 CNN 和 RNN+GAN 模型,其准确率、召回率、$F1$ 分数和 ROC AUC 均略低一些。SVM 在处理非线性问题时能力有限,而网络流量数据往往具有复杂的非线性特征。

(2)在 KDD Cup 99 数据集上,RNN+GAN 模型的准确率、召回率、$F1$ 分数和 ROC AUC 均接近或

达到了 0.95 以上，表明模型具有较好的分类性能和泛化能力。在 CICIDS2017 数据集上，虽然各项指标略有下降，但仍然保持在较高的水平，说明模型在现代网络环境中也具有一定的适用性。

4.3　实验结果与分析

4.3.1　准确率(Accuracy)评估与分析

为了全面评估不同单模型(SVM、CNN、RNN、GAN)和组合模型(RNN+CNN、RNN+GAN、CNN+GAN)在准确率方面的表现，在 KDD Cup 99 和 CICIDS2017 两个常用的网络流量数据集上进行了实验，结果见表 2。

表 2　不同模型在两个数据集上的准确率

Table 2　Accuracy of different models on two datasets

模型	KDD Cup 99	CICIDS2017
SVM[23]	0.880	0.870
CNN[23]	0.860	0.810
RNN	0.980	0.955
GAN	0.978	0.952
RNN+CNN	0.983	0.960
RNN+GAN	0.985	0.962
CNN+GAN	0.981	0.957

如表 2 所示，在所有模型中，RNN+GAN 组合模型在两个数据集上都取得了最高的准确率。在 KDD Cup 99[3] 数据集上，RNN+GAN 的准确率为 0.985，比单一模型如 SVM(0.975)和 CNN(0.982)都要高。在 CICIDS2017 数据集上，RNN+GAN 的准确率为 0.962，同样优于其他单模型和组合模型。

4.3.2　精确率(Precision)评估与分析

为了全面评估不同单模型(SVM、CNN、RNN、GAN)和组合模型(RNN+CNN、RNN+GAN、CNN+GAN)在精确率方面的表现，在两个常用的网络流量数据集 KDD Cup 99 和 CICIDS2017 上进行了实验，结果见表 3。

表 3　不同模型在两个数据集上的精确率

Table 3　Precision of different models on two datasets

模型	KDD Cup 99	CICIDS2017
SVM[23]	0.89	0.76
CNN[23]	0.87	0.84
RNN[24-25]	0.89	0.74
GAN	0.88	0.83
RNN+CNN	0.93	0.89
RNN+GAN	0.94	0.90
CNN+GAN	0.91	0.86

如表 3 所示，RNN+GAN 组合模型在两个数据集上都取得了最高的精确率。在 KDD Cup 99 数据集上，RNN+GAN 的精确率为 0.94，比单一模型如 SVM(0.89)和 CNN(0.87)都要高。在 CICIDS2017 数据集上，RNN+GAN 的精确率为 0.90，同样也超过了其他所有模型。

4.3.3　召回率(Recall)评估与分析

为了全面评估不同单模型(SVM、CNN、RNN、GAN)和组合模型(RNN+CNN、RNN+GAN、CNN+GAN)在召回率方面的表现，在两个常用的网络流量数据集 KDD Cup 99 和 CICIDS2017 上进行了实验，结果见表 4。

表 4　不同模型在两个数据集上的召回率

Table 4　Recall of different models on two datasets

模型	KDD Cup 99 召回率	CICIDS2017 召回率
SVM[23]	0.86	0.89
CNN[23]	0.83	0.83
RNN[24-25]	0.86	0.82
GAN	0.82	0.78
RNN+CNN	0.90	0.86
RNN+GAN	0.92	0.89
CNN+GAN	0.87	0.82

如表 4 所示，RNN+GAN 组合模型在两个数据集上都取得了最高的召回率。在 KDD Cup 99 数据集上，RNN+GAN 的召回率为 0.92，比单一模型 SVM(0.86)和 CNN(0.83)都要高。在 CICIDS2017 数据集上，RNN+GAN 的召回率为 0.89，同样也超过了其他所有模型。

4.3.4　$F1$ 分数($F1$-Score)综合评估与分析

为了全面评估不同单模型(SVM、CNN、RNN、GAN)和组合模型(RNN+CNN、RNN+GAN、CNN+GAN)在 $F1$ 分数方面的表现，在两个常用的网络流量数据集 KDD Cup 99 和 CICIDS2017 上进行了实验，结果见表 5。

表 5　不同模型在两个数据集上的 $F1$ 分数

Table 5　$F1$ Score of different models on two datasets

模型	$F1$ 分数	
	KDD Cup 99	CICIDS2017
SVM[23]	0.88	0.82
CNN[23]	0.85	0.83
RNN[24-25]	0.87	0.78
GAN	0.85	0.80
RNN+CNN	0.91	0.87
RNN+GAN	0.93	0.90
CNN+GAN	0.89	0.84

如表 5 所示，RNN+GAN 组合模型在两个数据

集上都取得了最高的 $F1$ 分数。在 KDD Cup 99 数据集上,RNN+GAN 的 $F1$ 分数为 0.93,比单一模型 SVM(0.88)和 CNN(0.85)都要高。在 CICIDS2017 数据集上,RNN+GAN 的 $F1$ 分数为 0.90,同样也超过了其他所有模型。

5 结束语

本文深入探讨了不同模型在计算机网络防御中的性能表现,通过模拟仿真实验对多种模型进行了全面的评估。从准确率(Accuracy)、精确率(Precision)、召回率(Recall)以及 $F1$ 分数($F1$ - Score)4 个核心指标出发,对实验结果进行了详尽的分析,主要结论如下:

(1)在准确率评估中,RNN+GAN 组合模型展现出了卓越的性能,在 KDD Cup 99 和 CICIDS2017 两个数据集上都取得了最高的准确率,分别为 0.985 和 0.962,说明 RNN+GAN 模型在整体分类任务上的优越性,能够准确地将正常网络流量与恶意网络流量区分开来,为网络安全提供了有力的保障。

(2)在精确率评估中,RNN+GAN 同样表现优异,取得了最高的精确率。在 KDD Cup 99 数据集上,RNN+GAN 的精确率为 0.94,在 CICIDS2017 数据集上为 0.90,均超过了其他所有模型。证明 RNN+GAN 模型在识别恶意网络流量时具有极高的准确性,误报率极低,对减少网络管理员的工作负担、提高网络防御效率具有重要意义。

(3)召回率评估进一步验证了 RNN+GAN 模型的优越性。该模型在两个数据集上都取得了最高的召回率,分别为 0.92 和 0.89。RNN+GAN 模型能够更全面地识别出网络攻击,有效减少漏报情况,对于确保网络安全至关重要。

(4)在 $F1$ 分数综合评估中,RNN+GAN 模型再次以最高的分数证明了其在综合性能方面的优势。在 KDD Cup 99 数据集上,RNN+GAN 的 $F1$ 分数为 0.93,在 CICIDS2017 数据集上为 0.90,均超过了其他所有模型。这一结果充分说明了 RNN+GAN 模型在减少误报和漏报之间取得了极佳的平衡,是计算机网络防御中的理想选择。

综上所述,在计算机网络防御中,RNN+GAN 组合模型在准确率、精确率、召回率以及 $F1$ 分数等关键指标上均表现出色,展现出强大的网络防御能力。不仅为未来的计算机网络防御研究提供了有价值的参考和指导,也为实际网络防御工作提供了新的思路和方向。

参考文献

[1] SUYKENS J. Support vector machines: A nonlinear modelling and control perspective[J]. European Journal of Control, 2001, 7(2/3): 311-327.

[2] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. ImageNet classification with deep convolutional neural networks [J]. Communications of the ACM, 2017, 60(6): 84-90.

[3] GOODFELLOW I, POUGET-ABADIE J, MIRZA M. Generative adversarial networks[C]//Proceedings of the Neural Information Processing Systems. NeurIPS, 2014: 2672-2680.

[4] 李晓. 人工智能技术在计算机网络防御中的应用研究[J]. 信息与电脑, 2023, 35(16): 212-214.

[5] 刘文元. 人工智能技术在计算机网络防御中的应用探索[J]. 信息记录材料, 2023, 24(3): 98-100.

[6] RAVIKUMARR C, NARESH B, PRASANNA P, et al. Exploring machine learning algorithms for robust cyber threat detection and classification: A comprehensive evaluation [C]//Proceedings of the International Conference on Intelligent Systems for Cybersecurity(ISCS). 2024: 1-5.

[7] 曹越. 人工智能技术在计算机网络安全中的应用研究[J]. 中国新通信, 2023, 25(17): 119-121.

[8] HUANG Z. Application research of artificial intelligence in computer network technology [C]//Proceedings of the 6th International Conference on Intelligent Computing, Communication, and Devices (ICCD). Piscataway, NJ: IEEE, 2023: 127031N.

[9] ALQARNI A A. Toward support-vector machine-based ant colony optimization algorithms for intrusion detection [J]. Soft Computing, 2023, 27(10): 6297-6305.

[10] 盛剑桥, 方圆, 张亮, 等. 粒子群算法优化 SVM 的无线网络安全状态检测方法[J]. 自动化技术与应用, 2022, 41(12): 55-58.

[11] LIU Ying, XUE Jinghao, LI Daxiang, et al. Image recognition based on lightweight convolutional neural network: Recent advances[J]. Image and Vision Computing, 2024, 146: 105037.

[12] 颜慧强, 李强, 季超凡. 基于卷积神经网络的安全防御模式研究[J]. 电信工程技术与标准化, 2021, 34(2): 89-92.

[13] ZHONG Ying, ZHU Yiran, WANG Ziran, et al. An Adversarial learning model for intrusion detection in real complex network environments [C]//Proceedings of the 15th International Conference on Wireless Algorithms, Systems, and Applications (WASA). Cham: Springer, 2020: 794-806.

[14] WANG Ping, LIN Hsiaochung, LIN Wenhui, et al. An efficient flow control approach for SDN-based network threat detection and migration using support vector machine[C]//Proceedings of the 13th IEEE International Conference on E-Business Engineering (ICEBE). Piscataway, NJ: IEEE, 2017: 56-63.

[15] AGARWAL N, KAUR A. Convolutional Neural Network-based anomaly detection for cyber security: A survey[C]//Proceedings of the 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). Piscataway, NJ: IEEE, 2023: 1738-1741.

[16] 杨丽, 吴雨茜, 王俊丽, 等. 循环神经网络研究综述[J]. 计算机应用, 2018, 38(S2): 1-6.

[17] DING Hongwei, SUN Yu, HUANG Nana, et al. TMG-GAN: Generative adversarial networks-based imbalanced learning for network intrusion detection[J]. IEEE Transactions on Information

Forensics and Security，2024，19：1156-1167.
[18]吴建胜，张文鹏，马垣. KDDCUP99 数据集的数据分析研究[J]. 计算机应用与软件，2014，31(11)：321-325.
[19] KURNIABUDI K，STIAWAN D，DARMAWIJOYO D，et al. CICIDS-2017 dataset feature analysis with information gain for anomaly detection[J]. IEEE Access，2020，8：132911-132921.
[20]ABADI M，ISARD M，MURRAY D G. A computational model for TensorFlow an introduction[C]//Proceedings of the 1st ACM SIGPLAN International Workshop on Machine Learning and Programming Languages. New York：ACM，2017：1-7.
[21] KINGMA D P，BA J L. Adam：A method for stochastic optimization[C]//Proceedings of the 3rd International Conference on Learning Representations. ICLR，2015：1-15.
[22]蓝新波，李冬睿. 径向基函数神经网络在网络安全预测中的应用[J]. 计算机测量与控制，2014，22(3)：836-838.
[23]曾勇. 基于深度神经网络的入侵检测研究[D]. 赣州：江西理工大学，2021.
[24]龙卓坤. 基于联合分布逼近与对比学习的网络流量异常分析研究[D]. 武汉：华中科技大学，2022.
[25]周静. 基于 DCGAN 和 Transformer 结合的网络流量异常检测方法研究[D]. 西安：西安理工大学，2023.