doi:10.11835/j.issn.1000.582X.2024.06.009

基于神经网络平滑聚合机制的恶意代码增量训练及检测

郭志民,陈　岑,李暖暖,蔡军飞,张　铮
(国网河南省电力公司 电力科学研究院,郑州 450000)

摘要:为保证恶意代码变种检测模型的时效性,传统基于机器(深度)学习的检测方法通过集成历史数据和新增数据进行重训练更新模型存在训练效率低的问题。笔者提出一种基于神经网络平滑聚合机制的恶意代码增量学习方法,通过设计神经网络模型平滑聚合函数使模型平滑演进,通过添加训练规模因子,避免增量模型因训练规模较小而影响聚合模型的准确性。实验结果表明,对比重训练方法,增量学习方法在提升训练效率的同时,几乎不降低模型的准确性。

关键词:恶意代码变种检测;增量学习;神经网络;模型聚合
中图分类号:TP391　　**文献标志码:**A　　**文章编号:**1000-582X(2024)06-086-08

Malware incremental training and detection method based on neural network smooth aggregation mechanism

GUO Zhimin, *CHEN Cen*, *LI Nuannuan*, *CAI Junfei*, *ZHANG Zheng*
(State Grid Henan Electric Power Research Institute, Zhengzhou 450000, P. R. China)

Abstract: To ensure the timeliness of malware variant detection models, traditional machine (deep) learning-based detection methods integrate historical and incremental data and retrain to update detection models. However, this approach often suffers from low training efficiency. Therefore, this paper proposes an incremental learning method based on a neural network smooth aggregation mechanism for detecting malware variants, facilitating the smooth evolution of detection models. The method introduces a training scale factor to prevent the decrement of accuracy in the aggregated incremental model due to small training scales. Experimental results show that the proposed incremental learning method can improve training efficiency while maintaining the accuracy of the detection model compared to the re-training method.

Keywords: malware variants detection; incremental learning; neural network; model aggregation

当今网络安全形势日益严峻,随着恶意软件及其变种的泛滥,未知变种已成为目前主要网络安全威胁之一。传统基于Hash特征码匹配的恶意代码检测方法受限于已知恶意软件Hash特征库的规模,难以应对海量未知变种威胁;另一方面,传统基于规则匹配的恶意代码检测方法在应对海量未知变种时,需要依赖专业知

收稿日期:2022-05-12
基金项目:国家电网有限公司总部科技项目资助(5700-202024193A-0-0-00)。
Supported by the Science and Technology Project of State Grid Corporation of China(5700-202024193A-0-0-00).
作者简介:郭志民(1977—),男,教授级高级工程师,主要从事信息安全方向研究,(Tel)13838273251;(E-mail)zhimin.guo@163.com。

识且耗费大量人力不断提取覆盖变种特征的新型规则,故同样不适用于海量恶意代码未知变种检测。不少学者提出基于机器学习的恶意代码未知变种检测方法[1-12]。基于机器学习的恶意代码未知变种检测方法通过自适应提取特征并构建模型,无须人工提取规则,极大提升恶意代码未知变种检测效率,且扩大恶意代码未知变种检测的范围,备受学术界和工业界关注。

然而,受限于有限被正确标记的恶意/良性代码样本,需要不断采集和标注样本数据,基于机器学习方法构建恶意代码变种检测模型的精度和召回率存在一定局限。随着恶意代码变种不断演进,恶意代码变种检测模型存在概念漂移问题,即检测模型存在一定时效性,为此,需要不断新增数据样本训练更新检测模型。但恶意代码变种检测模型的训练方法耗费大量时间开销[8],难以通过重训练的方式快速更新检测模型,使实时更新检测模型成为新的技术挑战。

针对上述问题,笔者提出一种基于神经网络平滑聚合机制的恶意代码增量训练及检测方法。通过设计神经网络平滑聚合机制,提出神经网络模型增量更新方法,结合已提取的恶意代码特征,构建恶意代码增量训练模型,提升恶意代码检测模型训练效率及检测时效。本文的主要贡献包括:1)提出一种基于神经网络平滑聚合机制的恶意代码增量训练及检测方法,通过构造操作码二元组共生概率矩阵,设计神经网络模型增量更新机制,并基于卷积神经网络增量训练恶意代码检测模型,提升恶意代码检测模型训练效率及检测时效;2)设计一种神经网络平滑聚合机制和聚合函数,引入历史模型偏重系数和训练规模因子,实现神经网络模型增量更新;3)实验结果表明:时间开销方面,提出的恶意代码增量训练及检测方法训练速度相较于传统重训练方法提升约 6 倍,同时检测时间开销<0.001 s;准确率方面,对比若干机器学习检测模型,本文方法的检测精度和召回率均有一定提升。

1　国内外研究现状

基于机器学习的恶意代码变种检测方法近几年一直是学术界研究热点,目前有不少学者提出基于机器(深度)学习方法,针对操作码语义特征、API行为特征等恶意代码变种检测方法。文献[1]采用卷积自编码器对较长操作码序列进行压缩编码,并采用动态递归神经网络训练模型和检测。文献[2]针对加密、混淆处理的恶意代码变种,提取恶意代码纹理图像特征,采用区域卷积神经网络对其进行识别。文献[3]提取恶意代码 API、权限等特征,采用基于汉明距离的 K 近邻算法计算未知样本与已知样本的相似度,判别未知样本类别。文献[4]采用决策树算法对恶意代码家族进行分类,并计算 IP 地址的加权风险值。文献[5]提出一种混合深度学习框架检测医疗物联网环境中的恶意代码。文献[6]首先构造恶意代码灰度图像并提取灰度图像特征,采用改进的卷积神经网络训练恶意代码检测模型。文献[7]采用隐马尔科夫链表征恶意代码 API 调用行为,并采取马尔科夫链匹配模型辨别未知样本与已知恶意样本的匹配程度。文献[8]提取恶意代码操作码的 n-gram 特征和 API 调用的频谱特征,采用卷积神经网络和 BP 神经网络训练构建恶意代码特征迁移集成学习模型。其他类似的工作提取不同的恶意代码特征或采用不同机器学习方法构造恶意代码变种检测模型[9-14]。

尽管上述研究在提升检测精度和召回率方面取得显著进展,但应用于工业界实际场景仍存在一些问题,例如,如何提升样本标注效率和正确性,不断新增样本情况下模型如何高效更新检测模型等问题,特别是关于检测模型增量学习方面的研究较少。因此,文本提出一种基于神经网络平滑聚合的恶意代码变种增量训练和检测方法,提升检测模型的训练更新效率确保检测模型的时效性。

2　基于神经网络平滑聚合的恶意代码增量训练及检测方法

2.1　问题描述

工业界不断从互联网、物联网、移动网中采集大量恶意/良性代码样本,但样本标注耗时耗力,受限于被正确标注的样本数量,使基于机器学习方法构建的恶意代码变种检测模型的精度和召回率存在一定限制,需要源源不断标注样本以扩充训练集规模,不断更新检测模型。不仅如此,随着恶意代码变种不断演进,恶意代码变种检测模型存在一定时效性,需要利用最新的样本不断更新检测模型,避免概念漂移问题。上述问题的解决依赖于恶意代码变种检测模型实时更新,然而,基于机器学习的检测模型训练方法耗费大量的时间开

销,难以通过重训练的方式快速更新检测模型。研究采取增量训练方式以快速更新检测模型,但增量训练仍然存在准确性下降或时效性不足等挑战。

2.2 总体方案

笔者提出一种基于神经网络平滑聚合机制的恶意代码增量训练及检测方法。采用Bi-gram模型提取恶意/良性代码特征,采用卷积神经网络作为训练检测模型的分类器,通过设计神经网络平滑聚合机制,提出神经网络模型增量更新方法,并基于该方法结合已提取的恶意代码特征,构建恶意代码增量训练模型,利用持续更新的检测模型对未知恶意软件变种进行检测,以提升恶意代码检测模型训练效率及检测时效性,总体方案如图1所示。

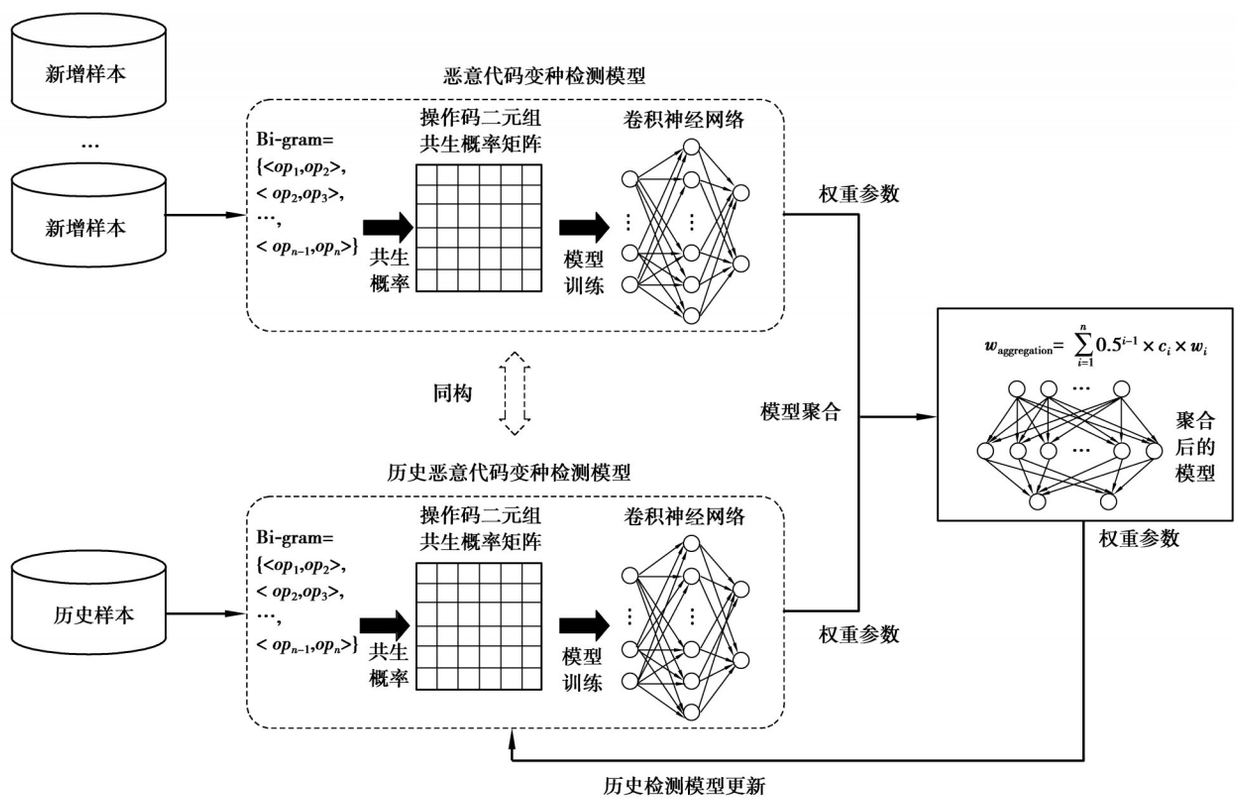

图1 总体方案

Fig. 1 The Architecture of Our Method

2.3 特征提取

Bi-gram模型是目前提取恶意代码特征的主流方法之一[8,13]。研究采用Bi-gram模型提取恶意/良性软件操作码二元组特征,以表示样本中两两操作之间的局部语义关系。首先,采用IDA Pro提取恶意/良性软件的操作码序列,令 $OP=\{op_1,op_2,...,op_n\}$ 为操作码序列,其中,op_i 表示序列中第个 i 操作码。然后,提取两两相邻操作码构成操作码二元组特征 Bi-gram $=\{<op_1,op_2>,<op_2,op_3>,...,<op_{n-1},op_n>\}$,并计算操作码二元组的共生概率,以表示恶意代码局部语义关系。操作码二元组及其共生概率矩阵作为输入卷积神经网络的特征向量,用于训练检测模型。

2.4 基于卷积神经网络的检测模型构建

现有恶意代码变种智能检测技术主要通过采用的机器(深度)学习方法包括K近邻、支持向量机、卷积神经网络训练大量已正确标注的恶意代码变种样本。对于恶意代码Bi-gram模型表征,卷积神经网络因能提取操作码之间的关联特征,可较好地表征代码局部语义信息。因此,基于卷积神经网络设计恶意代码变种检测模型,卷积神经网络包含5层,如图2所示:输入层、卷积层、池化层、全连接层、输出层。输入层输入操作码二元组共生概率矩阵;卷积层采用尺寸为3*3、5*5的卷积核对共生概率矩阵进行内积运算提取卷积层特征图;

池化层采用2*2的平均池化核对卷积层特征图进行压缩,形成池化层特征图。全连接层采用ReLU函数连接池化层特征图,ReLU函数如公式(1)所示,并采用Softmax函数全连接输出层,Softmax函数如公式(2)所示,其中:$\boldsymbol{x}$表示上一层层输入的特征向量;$\boldsymbol{w}$表示上一层与当前层的连接权重向量,输出层输出恶意/良性类别的置信度。

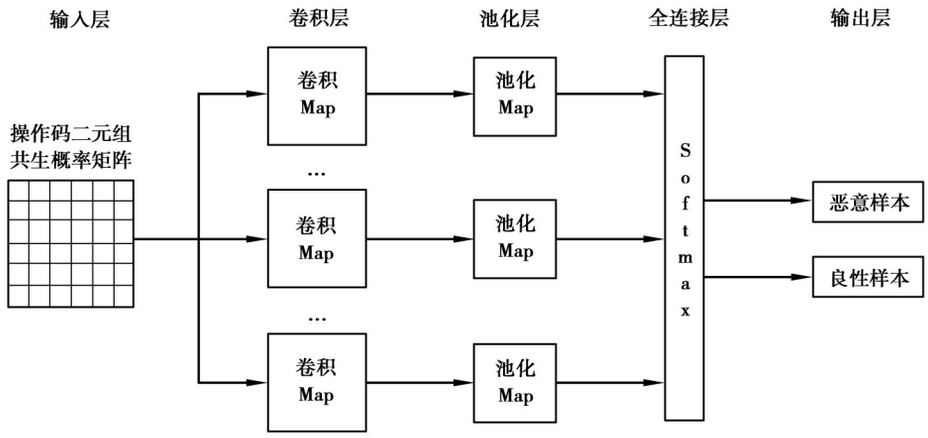

图2　卷积神经网络架构

Fig. 2　The Architecture of Our Convolutional Neural Network

$$\mathrm{ReLU}(\boldsymbol{w}\cdot\boldsymbol{x})=\max(0,\boldsymbol{w}\cdot\boldsymbol{x}), \tag{1}$$

$$\mathrm{Soft\,max}(\boldsymbol{w}\cdot\boldsymbol{x})=\frac{e^{\boldsymbol{w}\cdot\boldsymbol{x}}}{\sum e^{\boldsymbol{w}\cdot\boldsymbol{x}}}。 \tag{2}$$

研究采用梯度下降法训练恶意代码检测模型,根据卷积神经网络模型计算的误差反向传播修正模型中的权值,损失函数采用交叉熵如公式(3)所示,其中:Loss表示损失函数;y表示样本实际标签(0表示良性代码/1表示恶意代码),根据公式(4)迭代更新卷积神经网络权值参数

$$\mathrm{Loss}(\boldsymbol{w}\cdot\boldsymbol{x})=-(y\cdot\mathrm{Softmax}(\boldsymbol{w}\cdot\boldsymbol{x})+(1-y)\cdot(1-\mathrm{Softmax}(\boldsymbol{w}\cdot\boldsymbol{x}))), \tag{3}$$

$$\Delta\boldsymbol{w}=\alpha\cdot\frac{\partial\mathrm{Loss}}{\partial\mathrm{Softmax}(\boldsymbol{w}\cdot\boldsymbol{x})}\cdot\frac{\partial\mathrm{Softmax}(\boldsymbol{w}\cdot\boldsymbol{x})}{\partial\boldsymbol{w}}, \tag{4}$$

其中:$\Delta\boldsymbol{w}$表示权重更新;$\alpha=0.1$表示步长。

2.5　基于神经网络模型平滑聚合的增量训练

为保证恶意代码变种检测模型的时效性,基于机器(深度)学习的检测方法通过集成历史数据和新增数据进行重训练以更新模型。由于上述基于卷积神经网络的恶意代码检测模型训练过程耗费大量时间开销,难以通过重训练的方式快速更新检测模型,因此,基于神经网络模型平滑聚合的增量训练方法提升恶意代码检测模型更新效率,通过设计神经网络模型平滑聚合函数使模型平滑演进,通过添加训练规模因子,避免增量模型因训练规模较小而严重影响聚合模型的准确性。该方法对增量数据基于Bi-gram模型提取操作码二元组矩阵,利用上述卷积神经网络训练增量检测模型。因为增量检测模型与历史检测模型同构,可以将增量检测模型的权重参数与历史检测模型权重参数聚合,形成新的检测模型,再将新检测模型的权重参数更新至历史检测模型中,兼顾历史模型准确性和增量模型时效性的优势。

尽管采取增量训练方式快速更新检测模型,但保障增量训练的准确性和时效性仍是需要解决的关键问题。随着数据不断新增,增量模型与历史模型不断聚合形成新的历史模型,因综合了更多数据训练模型使准确性更有保障,增量模型因训练最新数据确保模型的时效性。但受限于增量训练样本较少(过多则影响检测模型更新速度),增量模型的准确性相对历史模型较差,如果直接聚合增量模型和历史模型,则会造成聚合后的模型准确性降低。

因此,基于神经网络模型平滑聚合的增量训练方法设计神经网络模型平滑聚合函数,如公式(5)所示,其中:$w_{\mathrm{aggregation}}$表示聚合后的检测模型权重参数;w_i表示历史前i次的增量训练模型的权重参数(如利用最新增

量数据训练出来的模型索引为1,则 $i=1$),利用增量数据训练得出卷积神经网络所有层的连接权重向量。通过不断衰减更早版本历史模型的偏重,使模型平滑演进,如历史前 m 次训练的增量模型偏重系数为 0.5^m。同时,通过添加训练规模因子 c_i,避免增量模型因训练规模较小而影响聚合模型的准确性,如公式(6)所示

$$w_{\text{aggregation}}=\sum_{i=1}^{n}0.5^{i-1}\cdot c_i\cdot w_i\ , \tag{5}$$

$$c_i=\frac{N_i}{N_1}\ , \tag{6}$$

其中:N_i 表示当前增量数据样本数量;N_1 表示第1次(历史前 N 次)增量训练的数据样本数量。最后,利用聚合后的权重参数更新检测模型,并对未知样本进行检测。

2.6 恶意代码变种检测

当检测未知代码样本时,首先提取未知样本的Bi-gram模型特征向量,将其输入至上述已训练好的最近一次聚合更新的卷积神经网络模型中。该检测模型通过多次增量式更新提升检测模型性能,通过提取代码样本的局部语义特征,并通过Softmax分类器进行检测输出置信度,对恶意/良性分类输出的置信度大小进行判定,选择置信度最大的分类作为判别结果(如果恶意类别的置信度>良性类别的置信度,即判定为恶意样本,反之则判定为良性样本)。

3 实验分析

3.1 实验环境

本文所有实验(恶意代码检测增量训练实验,以及用于对比的重训练实验)均在相同计算机软硬件环境和配置中进行,其中计算机CPU为Intel i5-3470 @ 3.20 GHz,内存容量为16.0 GB,操作系统为Ubuntu 16.04。

3.2 数据集和训练方法

实验所采用的恶意软件数据集来源于VxHeaven、Kaggle,其中,VxHeaven从若干用户计算机采集,包括17 000个恶意样本,10 300个良性样本。其中,80%的恶意/良性样本用于模型训练,20%的恶意/良性样本用于测试。所有训练样本均匀分成8个增量数据训练集,增量训练实验中,通过1次初始训练和7次增量训练;重训练实验中,整合全部历史数据集和新增的增量数据集进行训练,完成实验结果测试。

3.3 验证方法

所有实验均采取K-折交验证法,其中,K=5。评估指标包括训练时间开销、检测时间开销、准确率、精度和召回率,如公式(7)~(9)所示

$$\text{准确率}=\frac{TP+TN}{TP+TN+FP+FN}\ , \tag{7}$$

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

$$\text{召回率}=\frac{TP}{TP+FN}\ , \tag{9}$$

其中:TP 表示样本为恶意样本且检测正确;FP 表示样本为恶意样本且检测错误;TN 表示样本为良性样本且检测正确;FN 表示样本为良性样本且检测错误,精度表示模型判别恶意样本结果中正确结果的比例,召回率表示恶意样本中被模型正确检测出来的比例。

3.4 性能评估

本文利用测试数据集评估恶意代码检测模型增量学习方法的效率和准确性,同时,对比重训练方法的训练时间开销、精度和召回率,以验证提出方法相比于传统的重训练方法在模型训练速度方面具有显著优势,同时,尽可能不降低检测精度和召回率,实验最终结果如表1所示。

表1 性能评估指标和实验结果

Table 1 Performance Measure Metrics and Experimental Results

方法	训练时间/h	检测时间/s	精度/%	召回率/%
增量训练	6.4	<0.001	93.4	96.8
重训练	37.7	<0.001	94.6	95.1

时间开销结果表明:研究提出的恶意代码检测模型增量学习方法训练时间开销为6.4 h,检测时间开销<0.001 s。

对比重训练方法,增量学习方法在训练速度方面具有显著优势,加速比约为5.9倍,说明提出的方法能有利于提升恶意代码变种检测模型的更新效率。随着样本数量增加,增量训练时间开销基本保持水平。而重训练方法由于数据不断新增使得训练集规模不断增大,导致训练时间开销增加,如图3所示。

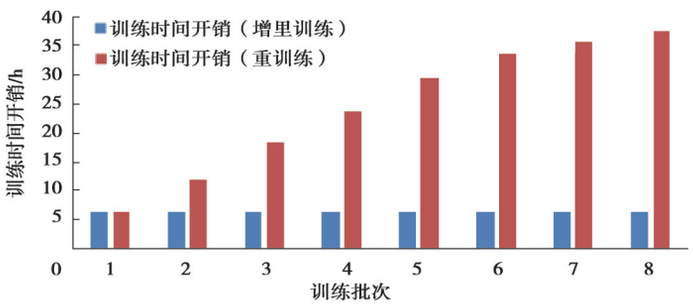

图3　训练时间开销对比实验结果

Fig. 3　Training Time Coast Comparison

准确性实验结果表明:提出的恶意代码检测模型增量学习方法检测精度=93.4 %、召回率=96.8 %。对比重训练方法,增量训练方法在新增数据训练后的精度和召回率几乎没有降低,说明研究方法在检测效率的同时保留了模型训练的准确性。随着增量训练次数增加,检测精度和召回率同时增加,说明增量训练的模型随着样本增加准确性提升,如图4所示。

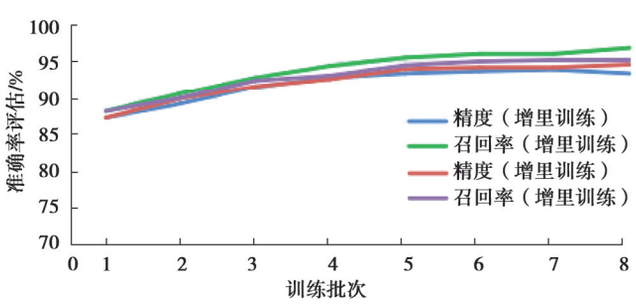

图4　准确性对比实验结果

Fig. 4　Accuracy Comparison

3.5　性能对比分析

通过对比几种常用的恶意软件检测方法的精度和召回率,进一步评估研究方法的准确性。对比方法均采用和研究相同的操作码二元组共生概率特征,分别采用不同的机器学习方法,包括支持向量机、BP神经网络和K近邻。实验结果表明,研究方法在精度和召回率指标上具有明显优势,如表2所示。

表2　性能对比分析结果

Table 2　Results of Performance Comparison　　%

方法	精度	召回率
本文方法	93.4	96.8
支持向量机	91.3	86.4
BP神经网络	89.1	90.5
K近邻	88.8	92.9

3.6 收敛性分析

通过对比增量学习模型收敛过程中训练集和测试集上检测准确率分析模型的收敛性，如图5所示，蓝色实线表示训练集的检测准确率，红色实线表示测试集的准确率，横坐标表示收敛迭代次数，纵坐标表示准确率。实验结果表明：1)随着迭代次数增加，模型准确率不断上升，且训练集收敛至100%，说明模型收敛性良好；2)测试集上的准确率和训练集上的准确率接近，且上升趋势几乎一致，说明模型并未出现过拟合现象。

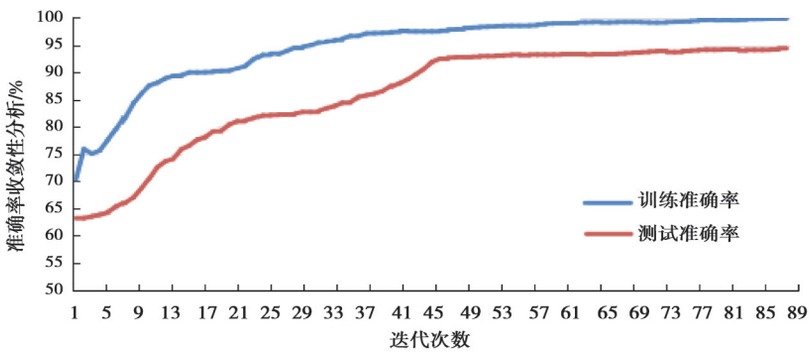

图5 收敛性分析

Fig. 5 convergence Analysis

3.7 训练规模因子分析

研究添加训练规模因子c_i，当增量训练数据规模较小时，增量模型相对历史模型权重较小，避免增量模型因训练规模较小(过拟合导致增量模型准确性下降)影响聚合模型的准确性。通过降低第8次增量训练数据规模，测试增量模型聚合后的准确性，实验结果如图6所示。尽管增量训练的数据规模降低，增量模型聚合后的准确性未受到明显影响，反映增量训练方法的稳健性。

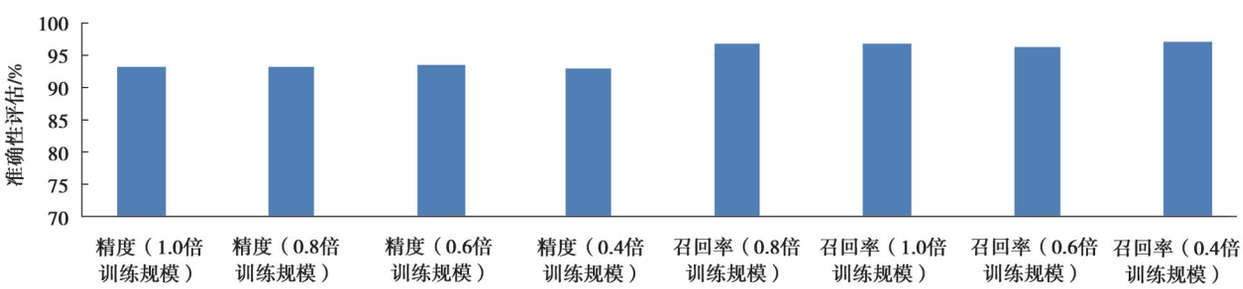

图6 训练规模因子分析实验结果

Fig. 6 Evaluation of incremental training scale

4 结束语

笔者提出一种基于神经网络模型平滑聚合机制的恶意代码增量训练及检测方法，提升恶意代码检测模型的训练性能，保障检测模型的准确性。该方法是基于神经网络模型平滑聚合的增量训练方法，减少模型训练时间开销的同时保障模型时效性，尽可能不降低模型训练的准确性。最后，对提出的恶意代码检测模型增量训练方法进行实验分析，结果表明，研究方法相比于机器学习重训练方法在训练速度方面具有明显优势，且几乎不降低检测的精度和召回率。

参考文献

[1] Jeon S, Moon J. Malware-detection method with a convolutional recurrent neural network using opcode sequences[J]. Information Sciences, 2020, 535: 1-15.

[2] Zhao Y T, Cui W J, Geng S N, et al. A malware detection method of code texture visualization based on an improved faster

RCNN combining transfer learning[J]. IEEE Access, 2020, 8: 166630-166641.

[3] Taheri R, Ghahramani M, Javidan R, et al. Similarity-based android malware detection using Hamming distance of static binary features[J]. Future Generation Computer Systems, 2020, 105: 230-247.

[4] Usman N, Usman S, Khan F, et al. Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics[J]. Future Generation Computer Systems, 2021, 118: 124-141.

[5] Khan S, Akhunzada A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT)[J]. Computer Communications, 2021, 170: 209-216.

[6] Bakour K, Ünver H M. DeepVisDroid: android malware detection by hybridizing image-based features with deep learning techniques[J]. Neural Computing and Applications, 2021, 33(18): 11499-11516.

[7] Suaboot J, Tari Z, Mahmood A, et al. Sub-curve HMM: a malware detection approach based on partial analysis of API call sequences[J]. Computers & Security, 2020, 92: 101773.

[8] Zhang J X, Qin Z, Yin H, et al. A feature-hybrid malware variants detection using CNN based opcode embedding and BPNN based API embedding[J]. Computers and Security, 2019, 84(C): 376-392.

[9] 陈志锋, 李清宝, 张平, 等 . 基于数据特征的内核恶意软件检测[J]. 软件学报, 2016, 27(12): 3172-3191.
Chen Z F, Li Q B, Zhang P, et al. Data characteristics-based kernel malware detection[J]. Journal of Software, 2016, 27(12): 3172-3191.(in Chinese)

[10] 杨欢, 张玉清, 胡予濮, 等 . 基于多类特征的Android应用恶意行为检测系统[J]. 计算机学报, 2014, 37(1): 15-27.
Yang H, Zhang Y Q, Hu Y P, et al. A malware behavior detection system of android applications based on multi-class features [J]. Chinese Journal of Computers, 2014, 37(1): 15-27.(in Chinese)

[11] 冀甜甜,方滨兴,崔翔,等 . 深度学习赋能的恶意代码攻防研究进展[J]. 计算机学报,2021,44(4): 669-695.
Ji T T, Fang B X, Cui X, et al. Research on deep learning-powered malware attack and defense techniques[J]. Chinese Journal of Computers, 2021, 44(4): 669-695.(in Chinese)

[12] 杨吉云, 陈钢, 鄢然, 等 . 一种基于系统行为序列特征的Android恶意代码检测方法[J]. 重庆大学学报, 2020, 43(9): 54-63.
Yang J Y, Chen G, Yan R, et al. An android malware detection method based on system behavior sequences[J]. Journal of Chongqing University, 2020, 43(9): 54-63.(in Chinese)

[13] 李苑, 王国胤, 李智星, 等 . 基于序列注意力机制的卷积神经网络异常检测[J]. 郑州大学学报(理学版), 2019, 51(2): 17-22.
Li Y, Wang G Y, Li Z X, et al. A sequential attention based convolutional neural network for anomaly detection[J]. Journal of Zhengzhou University (Natural Science Edition), 2019, 51(2): 17-22.(in Chinese)

[14] Kudugunta S, Ferrara E. Deep neural networks for bot detection[J]. Information Sciences, 2018, 467: 312-322.

（编辑　侯　湘）