基于 DAPA 的卷积神经网络 Web 异常流量检测方法*

高胜花[1],李世明[1,2],李秋月[1],於家伟[1],郑爱勤[1]
(1.哈尔滨师范大学 计算机科学与信息工程学院,黑龙江 哈尔滨 150025;
2.上海市信息安全综合管理技术研究重点实验室,上海 200240)

摘　要:针对 Web 攻击流量检测问题,提出一种基于动态自适应池化算法(Dynamic Adaptive Pooling Algorithm,DAPA)的卷积神经网络模型。首先将数据集中每一条请求流量进行剪裁、对齐、补足等操作,生成一系列 50×150 的矩阵数据 A 作为输入,然后搭建基于动态自适应的卷积神经网络模型去进行异常流量检测,使之可以根据特征图的不同,动态地调整池化过程,在网络结构中添加 Dropout 层来解决流量特征提取过程中的过拟合问题。实验表明,该方法比未使用动态自适应池化的方式精确度提升了 1.2%,损失值降低了 2.6%,过拟合问题也得到了解决。

关键词:异常流量检测;卷积神经网络;动态自适应池化
中图分类号:TP393　　**文献标识码**:A　　DOI:10.19358/j.issn.2096-5133.2020.02.002
引用格式:高胜花,李世明,李秋月,等.基于 DAPA 的卷积神经网络 Web 异常流量检测方法[J].信息技术与网络安全,2020,39(02):8-12.

A convolutional neural network Web abnormal flow detection method based on DAPA

Gao Shenghua[1],Li Shiming[1,2],Li Qiuyue[1],Yu Jiawei[1],Zheng Aiqin[1]
(1.College of Computer Science and Information Engineering,Harbin Normal University,Harbin 150025,China;
2.Shanghai Key Laboratory of Information Security Management Technology Research,Shanghai 200240,China)

Abstract:Aiming at the problem of Web attack traffic detection,a convolutional neural network model based on Dynamic Adaptive Pooling Algorithm (DAPA) was proposed. Firstly,each request traffic in the data set is trimmed,aligned,and complemented to generate a series of 50 × 150 matrix data A as input. Then,a dynamic adaptive convolutional neural network model built to detect abnormal traffic can adjust the pooling process dynamically according to different feature maps,and a Dropout layer can be added to the network structure to solve the problem of over-fitting in the flow feature extraction process. Experiments show that the method has an accuracy improvement of 1.2%,a loss value of 2.6%,and an over-fitting problem is solved compared with the method without using dynamic adaptive pooling.

Key words: abnormal flow detection;convolutional neural network;dynamic adaptive pooling

0　引言

在网络空间信息安全领域,网络流量异常检测对于保障网络的正常运行和网络的安全起着至关重要的作用[1]。随着网络服务应用数据巨增,Web 服务器遭受的攻击数量越来越多,攻击类型也越来越复杂,为保证向用户提供持续、安全和可靠的应用服务,需要实时检测出 Web 服务中的异常流量。现有的 Web 异常流量检测方法大多数为误用检测或是基于传统的机器学习算法检测[2];误用检测是根据已知攻击行为为主要特征,将入侵行为与正常行为根据已知特征加以区分来实现入侵行为的检测,该类方法效率高且误报率低,但只能发现已知的入侵类型,漏报率较高,特征的维护多采用人工方式完成。传统机器学习检测算法依靠手工提取流量中的特征,人为干预较严重。

1 相关工作

网络异常流量的检测是保障网络安全至关重要的防御步骤。文献[3]提出了一个可以普遍适用的入侵检测框架,该框架能够检测真实世界的僵尸

*基金项目:上海市信息安全管理技术研究重点实验室开放课题(AGK2015003)

网络,具有非常低的假阳性率。文献[4]建立了一个流量检测系统 MadTracer,自动生成检测规则,利用检测 Web 流量来判断服务是否包含不正当广告。实验结果表示 MadTracer 检测准确率达到了 95%,但只能检测已有的攻击类型。文献[5]针对 HTTP 异常流量检测问题,在原始数据的基础上与经验特征工程相结合的思想提出一种深度混合结构神经网络,所提方法检测效果有较明显提升,准确率可达 98.1%,但需要依赖人的经验特征,存在人为误差。文献[6]将深度学习应用到工控系统当中,将流量转换成灰度图,用构造好的灰度图去进行模型训练,对数据进行实时的异常检测,并做出相应的安全预防,实验结果显示精确度达到 97.88%。文献[7]搭建基于 SPP 卷积神经网络模型去进行 Web 攻击检测,解决传统模型只能处理固定大小输入的问题,但不能根据特征图的不同,动态地调整池化过程。

针对上述文献在异常流量检测中存在的问题,本文在传统的卷积神经网络基础上,构建基于动态自适应池化(Dynamic Adaptive Pooling Algorithm, DAPA)的卷积神经网络 Web 异常流量检测模型,可以根据特征图的不同,动态地调整池化过程,并在全连接层后连接了一个 Dropout 层,解决模型在流量特征提取过程中存在的过拟合问题,提高了模型的泛化能力。

2 Web 异常流量检测模型设计

目前,业界网络异常行为检测方法从原理上来说大约有如下几种分类,如表 1 所示。

表 1 网络异常检测方法分类

方法分类	特点
基于分类	按照检测粒度,确定具体需要分类的数量和类别
基于统计	给出的数据服从某种概率分布,利用各种数理统计相关技术
基于聚类	无监督检测方法,无需标注数据
基于信息论	利用网络流量数据集的特征,例如熵、信息增益等

本文采用基于分类方法中的二分类,搭建基于动态自适应池化的卷积神经网络模型,用该模型将数据流量划分为异常或正常。

2.1 Web 攻击检测框架

Web 攻击检测框架分为两个阶段,如图 1 所示。

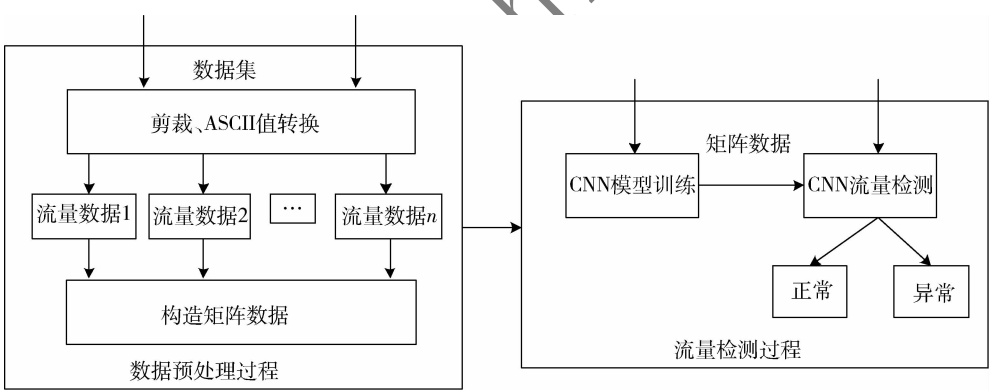

图 1 异常流量检测框架

第一阶段:数据预处理,进行流量捕获,获得数据集,对数据集中每一条请求流量进行剪裁、对齐、补足生成一系列 50 × 150 的矩阵数据,矩阵数据作为输入;

第二阶段:使用动态自适应池化卷积神经模型进行异常网络流量检测。

2.2 动态自适应池化 CNN 模型

动态自适应池化卷积神经网络模型如图 2 所示,异常流量检测过程中,流量数据转换成矩阵数据后,作为模型的输入。池化是对流量特征进行二次提取,需对池化域的流量特征进行归纳和计算,在全连接层后添加 Dropout 层。

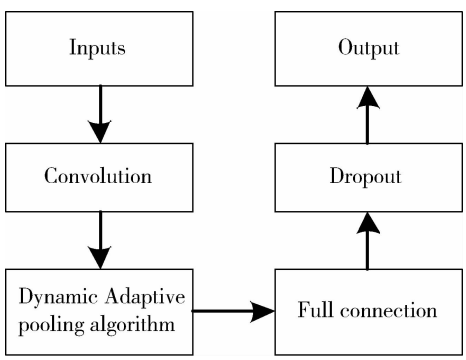

图 2 CNN 结构框架

2.2.1 动态自适应池化

池化是一种降采样的方法,池化层直接计算池化窗口内元素的特征值,设 $\boldsymbol{F}$ 为卷积层输入的流量矩阵,池化域为 $c \times c$ 的矩阵 $\boldsymbol{P}$,b_2 为偏置,$\boldsymbol{S}$ 为得到的子采样特征矩阵,池化过程移动步长设成 c,本文以最大二均值池化为基础,其表达式为:

$$\boldsymbol{S}_{ij} = \frac{1}{2} \operatorname*{sum}_{i=1,j=1}^{c} M_2(\boldsymbol{F}_{ij}) + b_2 \tag{1}$$

式(1)是在最大池化的基础上改进的,当一些影响因素的值较大时,使用最大池化,会降低流量矩阵特征的提取,所以本文池化时会选取最大的两个元素求和,并取和的平均值作为子采样的特征值。

动态自适应池化模型以最大二均值池化为基础进行改进与优化,最大池化模型和平均值池化模型在对流量特征图进行二次提取的时候,都很难取得较好的效果,因此提出了动态自适应池化算法,其算法表达式为:

$$\boldsymbol{S}_{ij} = \frac{u}{2} \operatorname*{sum}_{i=1,j=1} M_2(\boldsymbol{F}_{ij}) + b_2 \tag{2}$$

其中 u 为池化因子,如式(3)所示[8]:

$$u = p \frac{a(v_{\max} - a)}{v_{\max}^2} + \theta \tag{3}$$

其中 a 为流量特征图中除最大和第二大两个特征值外所有元素的平均值,$v_{\max}$ 为流量特征图中最大和第二大的两个特征值的平均值,θ 为校正误差项,p 为特征系数。流量特征图的不同会导致池化因子的取值不同,池化因子会动态调整来达到最优。池化因子取值范围为 $\mu \in (0,1)$,可以同时兼顾最大二均值池化和平均池化,在异常流量特征提取时既不会导致精度丢失过高,也降低了最大池化忽略其他较大因素时产生的影响。

2.2.2 CNN 中的 Dropout 层设计

本模型在异常流量特征提取过程中存在过拟合问题,其表现为错误检测率在训练集上非常低而在测试集上却较高,目前解决该问题的方法主要有正则化、剪枝处理、提前终止迭代、Dropout 等。

因 Dropout 具有较好的泛化能力和鲁棒性,故本模型采用 Dropout[9] 来解决过拟合问题。当每个神经元都去记录流量特征的时候就会让特征信息被过度地记录,导致仅仅记住了训练集上固定的特征。而 Dropout 层只有部分的神经元参与权值更新,弱化了神经元之间的相互影响,从而有效预防了固定特征被学习记录的问题。

3 实验结果与分析

3.1 实验数据集

实验数据采用公开自动生成的数据集 HTTP CSIC2020[10],该数据集包含上万条 Web 请求数据,由西班牙研究委员会(CSIC)信息安全研究所制作。数据集包含正常请求约 36 000 个,异常请求约 25 000 个。

将数据集标记为 Normal(training)、Normal(test)和 Anomalous(test),并分离成独立的 Web 请求文件。数据集包括各种攻击,主要攻击类型如表 2 所示。

表 2 攻击类型及其特点

攻击类型	攻击特点
SQL 注入	非法修改 SQL 语句,欺骗数据库服务器执行非授权的查询
缓冲区溢出	远程用户利用缓冲区溢出漏洞,非法获取系统特权
CRLF 注入	服务器未过滤攻击者输入的数据,直接放在头部,攻击者就可以通过注入\n\r(%0d%0a)控制 HTTP 返回头部
跨站脚本	黑客利用网站没有对用户提交数据进行转义处理,通过 HTML 注入篡改网页,插入恶意的脚本,在用户浏览网页时,控制网页浏览器
参数篡改	非法对客户端和服务器之间交换的参数修改

该数据集主要包括 GET、POST、PUT 三种类型数据,一个 Web 请求记录至少包含上述一种类型数据,且以该类型数据为边界符,在请求数据提取后,还需要对数据进行字符串分割,分割依据 HTTP 请求报文的格式规范进行,主要涉及 URL 地址解码,参数项、键值对、特殊符号的分割,得到每一条流量数据过后,对每一条请求流量进行裁剪、对齐、补足等操作,生成 50 × 150 的矩阵数据 A,所得矩阵数据 A 格式如图 3 所示,与数据处理前的数据流量作为

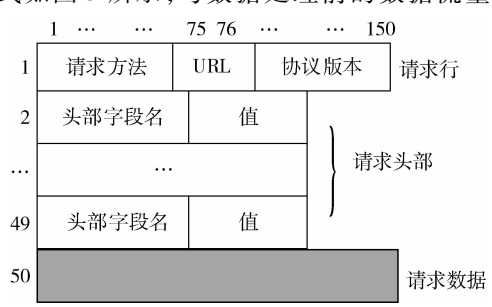

图 3 矩阵数据格式

输入相比,可以看出矩阵数据 A 更好地保留了流量数据原本的语序顺序和结构格式,使得数据流量的特征提取能够更加全面、更加精准。

3.2 实验结果与分析

实验环境为 Windows 10 操作系统、Python3.7.3 语言、TensorFLow 框架,计算机 CPU 为 Intel Core i5-4210u,内存 8 GB,硬盘空间为 2 TB,实验约 61 000 个矩阵数据,训练集与测试集比例为 9:1。

使用评价指标准确率和损失值对模型的检测结果进行评估,准确率计算如公式(4)所示,式中 TP(True Positives)和 TN(True Negatives)表示被正确划分为正常和异常的个数;FP(False Positives)和 FN(False Negatives)表示被错误划分为正常和异常的个数。准确率越高,检测效果越好。

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

该实验选择交叉熵作为本文的损失函数,因为交叉熵描述的是 2 个概率分布之间的距离,交叉熵函数计算如公式(5)所示,q 表示预测值概率分布,p 表示正确的概率分布。

$$H(p,q) = -\sum_{x} p(x)\log(q(x)) \tag{5}$$

实验使用两种检测方法进行对比,分别为:使用不包含 DAPA 的传统卷积神经与本文提出的基于 DAPA 的卷积神经网络进行实验对比,实验对比结果如表 3 所列,由表 3 可看出,使用了 DAPA 的卷积神经网络精确度比未使用 DAPA 的神经网络精确度提高了 1.2%,损失值降低了 2.6%。

表 3 实验结果

算法	精确度/%	损失值/%
DAPA-CNN	89.3	22.3
NDAPA-CNN	88.1	24.9

图 4 为加入 Dropout 技术前后及加入该技术时设置不同参数进行的对比实验图,模型中加入 Dropout 技术的目的是为了改善模型的过拟合问题。从图 4 中能够看出,当神经元占比数为 100% 时(即不加入 Dropout 技术)损失值最高,本模型会通过对训练数据的过度训练来降低损失值,从而出现过度拟合的现象;加入 Dropout 技术后,神经元占比数为 40% 时,损失值降低了 4.2%,精确度提高了 6%,所以本文选择设置参数为 0.4,改善模型的过拟合性。

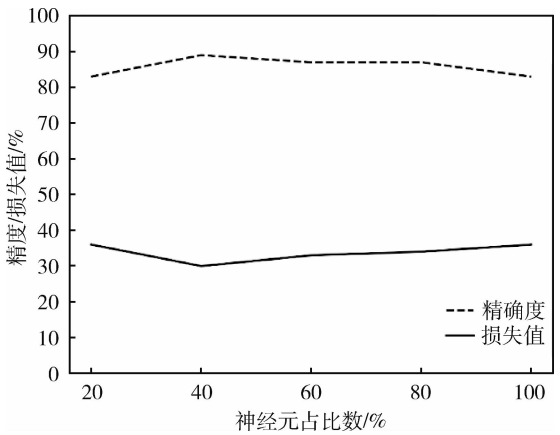

图 4 神经元占比实验图

本文进行了不同迭代次数的实验对比,模型在不同的迭代次数过程中会生成不同的一个个小网络,对每个算法进行迭代训练,模型每增加一次迭代次数,都会使神经元之间的组合产生新的变化,使得神经元不会组成固定组合对模型学习过程产生影响,使得参数均匀分布,实验结果如图 5 所示。

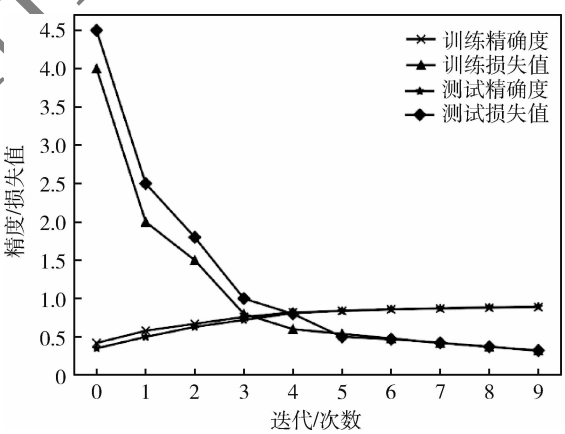

图 5 实验精确度和损失值

4 结论

本文针对 Web 攻击流量检测问题,提出了一种基于动态自适应池化的卷积神经网络异常流量检测模型,将数据集转换成矩阵数据作为模型输入,模型根据输入特征图的不同,动态自适应地调整池化过程,用 Dropout 层来解决模型中存在的过拟合问题。实验结果表明,使用了动态自适应池化模型的效果更好,过拟合问题也得到了改善。

参考文献

[1] 王伟. 基于深度学习的网络流量分类及异常检测方法研究[D]. 合肥:中国科学技术大学,2018.

[2] 张蕾,崔勇,刘静,等. 机器学习在网络空间安全研究中的应用[J]. 计算机学报,2018,41(9):1943-1975.

[3] GU G,PERDISCI R,ZHANG J,et al. BotMiner:clustering analysis of network traffic for protocol-and structure-independent botnet detection[C]. The 17th USENIX Security Symposium,2018:139-154.

[4] LI Z,ZHANG K,XIE Y,et al. Knowing your enemy:understanding and detecting malicious web advertising[C]. The 2012 ACM Conference on Computer and Communications Security,2012:674-686.

[5] 李佳,云晓春,李书豪,等. 基于混合结构深度神经网络的 HTTP 恶意流量检测方法[J]. 通信学报,2019,40(1):24-33.

[6] 张艳升,李喜旺,李丹. 基于卷积神经网络的工控网络异常流量检测[J]. 计算机应用,2019,39(5):1512-1517.

[7] 田俊峰,石伟. 一种基于卷积神经网络的 Web 攻击检测方法[J]. 小型微型计算机系统,2019,40(3):584-588.

[8] 刘万军,梁雪剑,曲海成. 不同池化模型的卷积神经网络学习性能研究[J]. 中国图象图形学报,2016,21(9):1178-1190.

[9] Constrained optimization using an evolutionary programming-based cultural algorithm[M]. Adaptive Computing in Design and Manufacture V. Berlin: Springer, 2002: 317-328.

[10] TORRANO-GIMNEZ C,PREZ-VILLEGAS A,ALVAREZ G. The HTTP dataset CSIC2010[EB/OL]. (2012-01-20)[2018-03-07]. http://www. isi. csic. es/dataset /2012-01-20/2018-03-07.

(收稿日期:2019-12-29)

作者简介:

高胜花(1997 -),女,硕士研究生,主要研究方向:网络与信息安全。

李世明(1976 -),通信作者,男,硕士,副教授,主要研究方向:网络空间安全、物联网技术、数据挖掘。E-mail:hsdlsm@ 163. com。

李秋月(1992 -),女,硕士研究生,主要研究方向:网络与信息安全。

版权声明