文章编号：2096-1472(2020)-05-27-03
DOI:10.19644/j.cnki.issn2096-1472.2020.05.008

恶意弹窗广告攻击检测技术的研究

孙冲冲，徐亚峰，卜东泰，韩港成，胥勋鹏，高 明

(徐州工程学院信息工程学院，江苏 徐州 221000)
✉1247477591@qq.com; 50002729@qq.com; 1169545234@qq.com;
609969059@qq.com; 1127635219@qq.com; 2249858875@qq.com

摘 要：恶意弹窗广告是一种强迫式的广告，这些广告给投放者带来巨大的利益，但是严重影响了用户体验，侵犯了用户权益，同时也带来很多安全隐患。恶意弹窗广告攻击检测系统采用C/S架构，服务端使用朴素贝叶斯算法根据训练集生成和更新训练结果，并利用训练结果对客户端发送的弹窗截图文本进行分类预测。客户端包括基础拦截、截图拦截以及主动拦截三个模块，主动拦截模块使用OCR技术将可疑弹窗截图转化为文本，然后把此文本传给服务端，服务端加载之前训练集产生的训练结果，利用朴素贝叶斯算法得到此文本的预测结果，客户端根据预测结果确定对此弹窗是否拦截。本系统实现了弹窗识别拦截的智能化，配置方便，交互界面易于使用。

关键词：弹窗广告；机器学习；朴素贝叶斯算法；拦截
中图分类号：TP315 **文献标识码**：A

Research on the Detection Technology of Malicious Pop-up Advertisements Attack

SUN Chongchong, XU Yafeng, BU Dongtai, HAN Gangcheng, XU Xunpeng, GAO Ming

(*College of Information Engineering*, *Xuzhou University of Technology*, *Xuzhou* 221000, *China*)
✉1247477591@qq.com; 50002729@qq.com; 1169545234@qq.com;
609969059@qq.com; 1127635219@qq.com; 2249858875@qq.com

Abstract: Malicious pop-up advertisements are imposed on users. These advertisements bring huge benefits to the publishers, but seriously affect user experience, infringe on user rights and interests, and also bring many security risks. The malicious pop-up advertisements attack detection system uses C/S (Client/Server) architecture. The server uses Naive Bayes algorithm to generate and update training results based on the training set, and uses the training results to classify and predict the pop-up screenshot text sent by the client. The client includes three modules: basic interception, screenshot interception, and active interception. The active interception module uses OCR (Optical Character Recognition) technology to convert the suspicious pop-up screenshot into text, and then transmits this text to the server. The server loads the training results generated by the previous training set. The naive Bayesian algorithm is used to obtain the prediction result of this text, and the client determines whether to block the pop-up window according to the prediction result. The system implements the intelligent identification and interception of the pop-up window, with convenient configuration and user-friendly interface.

Keywords:pop-up advertisements; machine learning; naive Bayesian algorithm; interception

1 引言(Introduction)

受到利益的驱使，很多恶意软件都捆绑了大量的广告。但是，以这种方式获利是不健康，不正当的，不利于互联网产业的正常发展。虽然目前有一部分拦截软件实现了恶意广告拦截的功能，但很多弹窗广告依赖用户识别，智能化程度不高。本项目就是在研究相应的检测技术的基础上，设计与实现一款高效率的智能恶意弹窗检测系统，扼制恶意广告泛滥的情况，营造良好的上网环境。

2 系统功能介绍(Introduction of system function)

本系统采用C/S(Client/Server，客户端/服务端)架构。客户端主要负责与用户的交互，同时具有轻量的数据处理任务；服务端主要负责用户数据处理。

基金项目：江苏省大学生创新创业训练项目(xcx2019030)。

2.1 客户端设计

本系统的客户端使用基于.NET Framework框架的C＃语言，采用WinFrom窗体作为交互界面，既保证了客户端的良好兼容性，也为用户提供了友好的交互方式。

客户端主要包含的功能有：基础拦截功能、截图拦截功能、主动拦截功能。基础拦截功能是指开启拦截后，拦截黑名单的程序；截图拦截功能是指根据用户选中的窗口，对相关应用加以拦截；主动拦截功能是指主动监控自动弹出的窗口，将此弹窗的文本信息给服务端后，根据服务端的返回预测结果决定对此弹窗是否拦截。

2.2 服务端设计

服务端部署在BCC(Baidu Cloud Compute，百度云服务器)上，提供了Socket(套接字)通讯服务和FTP(File Transfer Protocol，文件传输协议)服务，处理服务端和客户端之间的数据通信。

服务端包含的主要功能有：使用朴素贝叶斯算法根据训练集生成和更新训练结果，并利用训练结果对客户端发送的弹窗截图文本进行分类预测；收集客户端上传的弹窗图片，用以丰富训练集。

3 基础拦截功能(Basic interception function)

3.1 SQLite数据库的介绍

SQLite是世界上最广泛部署的SQL数据库引擎之一，它是一个进程内的库，实现了自给自足的、无服务器的、零配置的、事务性的SQL数据库引擎，具有轻量、速度快、稳定等特点[1]。SQLite的小巧稳定为本系统数据存储提供可靠支持。

3.2 基础拦截功能流程

当本系统的客户端软件运行并打开拦截功能后，将通过System.Diagnostics命名空间下的Process类获取当前进程，实时与黑名单以及白名单的应用比对，并结束在黑名单且不在白名单中的应用。

4 截图拦截功能(Screenshot interception function)

4.1 Win32 API

Win32 API是Microsoft Windows上预留的应用程序编程接口，得益于.NET Framework的灵活性，本系统可以通过c＃语言很便利地获取API接口，很好地实现了根据位置获取窗口句柄、直接获取目标窗口截图等功能[2,3]。

4.2 截图拦截流程

用户点击截图拦截按钮后，会立即生成一个与当前桌面相同的窗口，当用户单击后，通过调用Win32 API，获取此位置的窗口句柄，在用户点击确认按钮后，将应用加入黑名单。

5 主动拦截功能(Active interception function)

5.1 朴素贝叶斯算法

朴素贝叶斯算法(Naive Bayesian algorithm)基于概率论，是最广泛的机器学习分类算法之一。它在原本贝叶斯算法的基础之上，假定各特征相互独立，极大简化了算法的复杂性，提高了算法的使用效率。本系统将在文本分类阶段使用此算法，对文本加以分类。

贝叶斯公式：

$$P(A|B)=P(A)\cdot\frac{P(B|A)}{P(B)} \tag{1}$$

其中，我们把$P(A)$称作“先验概率”，$P(A|B)$称作后验概率，$\frac{P(B|A)}{P(B)}$称作“可能性函数”。

我们将A、B分别换成类别和特征，则表达式可写成：

$$P(\text{类别}|\text{特征})=P(\text{类别})\cdot\frac{P(\text{特征}|\text{类别})}{P(\text{特征})} \tag{2}$$

在本系统中，我们分别有恶意弹窗和正常窗口两种可分类的类别。在特征固定的情形下，我们即可通过比较P(恶意弹窗｜特征)与P(正常窗口｜特征)的大小判断特征所属的类别。因为P(恶意弹窗｜特征)与P(正常窗口｜特征)属于后验概率，所以两者并不便于直接比较。不过，我们可以将它们分别代入贝叶斯公式，将比较的目标变成比较$P(\text{恶意弹窗})\cdot\frac{P(\text{特征}|\text{恶意弹窗})}{P(\text{特征})}$与$P(\text{正常窗口})\cdot\frac{P(\text{特征}|\text{正常窗口})}{P(\text{特征})}$的大小。因为分母相同，所以我们只需比较$P$(恶意弹窗)$\cdot P$(特征｜恶意弹窗)与$P$(正常窗口)$\cdot P$(特征｜正常窗口)的大小即可[4,5]。

朴素贝叶斯算法假定了特征之间相互独立，所以很容易比较P(恶意弹窗)$\cdot P$(特征｜恶意弹窗)与P(正常窗口)$\cdot P$(特征｜正常窗口)的大小，从而确定类别。

朴素贝叶斯算法分类效率稳定，在文本数量较少时，依然会有较好的表现，同时对确实数据不敏感，适用性良好。相对于贝叶斯算法，由于朴素贝叶斯算法假设了属性之间相互独立，牺牲了一定的准确率[6]。

由于本系统所收集的训练样本较少，而朴素贝叶斯算法对少量的文本依然有较好的支持；同时，识别后文本的属性之间独立性较高，有效减少了属性之间相互独立的假设多带来的误差。

5.2 训练集

本系统将借助Sklearn库辅助模型训练，并实现训练集的保存和加载。Sklearn(Scikit-learn)是基于Python语言的机器学习库，它通过NumPy、SciPy和Matplotlib等Python库融合，高效地实现了几乎所有主流机器学习算法。

我们将收集到的恶意弹窗截图和正常软件截图分开置于两个文件夹里，其中两种截图各占50%；接着分别把两类截图使用OCR(Optical Character Recognition，光学字符识别)转换为文本。处理后的两类文本分开放置，共同作为训练集。

5.3 数据处理

(1)jieba分词

jieba是目前最好的Python中文分词库，它支持精确模式、全模式、搜索引擎模式这三种分词模式[7]。本系统的中文文档采用精确模式，配合stopword(停止词)的使用，对中文文本处理有很好的效果。

(2)One-Hot编码(独热码)

One-Hot编码使用二进制向量表示分类变量，在将分类值映射为整数值后，用二进制向量表示每个整数值。本系统中我们将文本中的词与词袋的词一一比较，若该词位于词袋中，则编码为1，否则编码为0。

(3)数据处理流程

首先加载由OCR识别后的文本，接着利用正则表达式匹配，去除文本中的非中文字符，然后用jieba分词，获得分割后的中文文本。获取分割后的文本后，我们将所有的文本及其类别的集合划分训练集和测试集，生成词袋。最后生成One-Hot编码，获得特征值。

5.4 使用朴素贝叶斯算法生成文本预测

获取数据集，在数据处理后，得到数据集的特征值集合；接着调用sklearn库中的MultinomialNB()方法，结合特征集合实例化分类器；最后调用sklearn库中的joblib，将训练的结果持久保存。

在服务端的socket模块获得待分类数据后，会将文本传入分类脚本。分类脚本在处理时，先通过joblib加载已经保存的训练结果，生成分类器。最后调用分类器的predict()方法，获得预测的分类结果，并回传socket通讯模块，文本预测流程如图1所示。

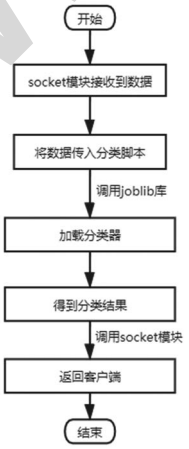

图1 文本预测流程图

Fig.1 Text prediction flowchart

5.5 主动拦截的实现

Hook(钩子)是windows中提供的一种用以替换DOS下“中断”的系统机制，它可以在系统调用某函数之前，提前捕获消息。在钩子捕获消息，获得控制权时后，便可以对该函数加以处理。在源码未知的情况下，可以通过钩挂相应的API函数，完成函数地址重写实现功能扩展[8]。

在本系统中，利用Hook获取了鼠标的单击事件。在客户端开启主动拦截功能后，主动拦截模块将不断监控桌面窗口的创建，每当用户未通过鼠标点击而弹出窗口时，便将此窗口的应用标为可疑应用程序，等待进一步的鉴定。

首先监控桌面应用程序，发现可疑应用程序后，调用Win32API获取可疑程序的截图，接着使用OCR得到可疑程序截图的文本内容，并将文本内容交给服务器进行文本预测；最后得到服务器返回的预测结果，并根据预测结果决定是否进行拦截，主动拦截流程如图2所示。

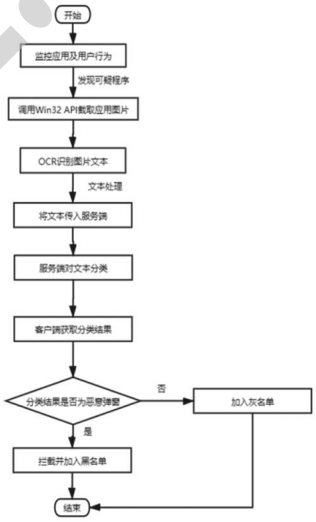

图2 主动拦截流程图

Fig.2 Active interception flowchart

如果客户端出现恶意弹窗广告，客户端传递此恶意弹窗的内容文本到服务端，服务端对此内容文本加以预测，如果预测的结果为：“pop”，就代表此窗口是恶意弹窗，客户端的预测如图3所示；客户端收到预测结果后，恶意弹窗广告被拦截，拦截后的效果如图4所示。

图3 服务端对弹窗截图内容的预测

Fig.3 Prediction of pop-up screenshot content by server

图4 恶意弹窗广告被拦截

Fig.4 Malicious pop-up advertisements blocked

6 结论(Conclusion)

本恶意弹窗广告攻击检测系统通过客户端与服务端之间通信，实现了智能化拦截。客户端为用户提供了良好的交互支持，界面友好易用。基础拦截功能、截图拦截功能和主动拦截功能互相配合，实现了较好的拦截效果。相较于其他的拦截软件，主动拦截功能的智能化大大提升了用户的使用体验。服务端为客户端可以提供可靠的数据处理支持。得益于朴素贝叶斯算法的高性能，本系统对服务器的性能要求不高，有良好的经济可行性。

参考文献(References)

[1] 邓杰海,全智龙,周红娟.基于C#与SQLite的银行财政非税收入管理软件的研发[J].电脑知识与技术,2017,13(10):74-75.

[2] Jefrey Richter.王建华,译.Windows核心编程[M].北京:机械工业出版社,2000.

[3] W.Richard Stevens.杨继张,译.第2卷进程间通信(第2版)[M].北京:清华大学出版社,2002.

[4] 刘秋阳,林泽锋,栾青青.基于朴素贝叶斯算法的垃圾短信智能识别系统[J].电脑知识与技术,2016,12(12):190-192.

[5] 邹晓辉.朴素贝叶斯算法在文本分类中的应用[J].数字技术与应用,2017(12):132-133.

[6] 郭勋诚.朴素贝叶斯分类算法应用研究[J].通讯世界,2019,26(01):241-242.

[7] 严明,郑昌兴.Python环境下的文本分词与词云制作[J].现代计算机(专业版),2018(34):86-89.

[8] 苏雪丽,袁丁.Windows下两种API钩挂技术的研究与实现[J].计算机工程与设计,2011,32(07):2548-2552.

作者简介：

孙冲冲(1998-)，男，本科生.研究领域：信息安全.

徐亚峰(1980-)，男，硕士，副教授.研究领域：网络工程.

卜东泰(1997-)，男，本科生.研究领域：软件工程.

韩港成(1997-)，男，本科生.研究领域：信息安全.

胥勋鹏(2000-)，男，本科生.研究领域：信息安全.

高　明(1998-)，男，本科生.研究领域：信息安全.

(上接第62页)

间内选择最优算法，也为后期模式识别和机器视觉相关应用的扩展研究奠定了基础。

参考文献(References)

[1] 张学军.基于Matlab图像处理的车牌号识别系统设计[J].信息通信,2018(07):36-38.

[2] 仲晓庆,蔡朝晖.基于MATLAB的几个图像处理实例[J].信息系统工程,2018(12):96-98.

[3] Zhao Jian-fei.Study on Shadow Processing Method Based on Background of Matlab Scans[C].2018 联合国际先进工程与技术研究国际会议论文集,2018:255-259.

[4] 张玉薇,杨建斌.一种便捷数字图像处理系统的MATLAB实现[J].信息记录材料,2019,20(02):40-42.

[5] 杨艳,夏福全,陈章宝.基于MATLAB GUI的Gabor滤波器数字图像处理实验平台设计[J].蚌埠学院学报,2019,8(02):57-60.

[6] 张新景,王勇,史颖刚.基于MATLAB GUI的图像处理演示系统[J].信息技术与信息化,2019(05):84-86.

[7] Ahmad Mohammadbeigi,Mohammad Rezaei,Naser Zohourian Sani,et al.Code and data on the processing of the pulsed-field gel electrophoresis images:A matlab script[J].Data in Brief,2020,28(28):21-25.

[8] 任鸿鹏.基于傅里叶变换的MATLAB图像处理[J].科技资讯,2019,17(16):11-12;14.

[9] 韩利利,田益民,齐千慧,等.基于MATLAB数字图像边缘检测算法的研究[J].北京印刷学院学报,2019,27(07):98-101.

[10] 王大海.基于Matlab的图像分析系统研究与设计[J].电子测试,2018(09):57-58.

[11] Pingping Jia.Application of Image Processing Technology based on Matlab[C].International Information and Engineering Association.Proceedings of 2018 International Conference on Data Processing,Artificial Intelligence,and Communications(DPAIC 2018).International Information and Engineering Association:计算机科学与电子技术国际学会(Computer Science and Electronic Technology International Society),2018:13-16.

[12] 魏润国,禹舜,胡东升,等.智能数字图像处理系统的设计与实现[J].电子设计工程,2018,26(16):160-164.

作者简介：

厉　俊(1999-)，男，本科生.研究领域：机器视觉与图像处理，信号与信息处理.