基于改进贝叶斯算法的文件监控系统研究*

周 亮
（中移铁通湖南分公司云数据支撑中心 长沙 412006）

摘 要 在互联网飞速发展的今天，计算机安全问题已经成为一个不可忽视的问题。传统的被动防御技术无法满足当前需求，主动防御应运而生。主动防御对病毒的行为进行分析，在病毒对系统造成无法预估的伤害之前作出处理，是目前研究的热点，而主动防御技术的基础就是文件监控。论文提出了基于行为分析的文件监控系统，该系统能够及时发现可疑程序的行为，并将这些行为通过行为分析算法进行分析评判。论文的行为分析算法在传统的朴素贝叶斯算法基础上提出加权思想，弥补了朴素贝叶斯假设特征变量之间不关联带来的偏差，提高了对文件行为判断的准确性。

关键词 主动防御；文件监控；行为分析；贝叶斯算法
中图分类号 TP311 **DOI**：10. 3969/j. issn. 1672-9730. 2018. 04. 022

Research on File Monitoring System Based on Improved Bayesian Algorithm

ZHOU Liang
（Cloud Data Support Center of China Mobile Tietong Hunan Branch, Changsha 412006）

Abstract With the rapid development of the Internet, the issue of computer security has become a problem that can not be ignored. The traditional passive defensive technology can not meet the current needs, active defense came into being. Active defense analyzes the behavior of the virus, deal with the virus before it can cause unpredictable damage to the system, and is the focus of current research, and the basis of active defense technology is file monitoring. This paper presents a document monitoring system based on behavior analysis, which can detect the behavior of suspicious program in time and analyze the behavior through behavioral analysis algorithm. In this paper, the behavior analysis of algorithm in the traditional naive Bayesian algorithm based on weighted thought, to make up for a simple Bayesian hypothesis deviation no correlation between characteristic variables, improve the accuracy of the judgment of file action.

Key Words active defense, file monitor, behavior analysis, bayes algorithm
Class Number TP311

1 引言

随着国际互联网络的发展，计算机联网数量在飞速增加，黑客、病毒和木马已经呈现出爆发式增长模式[1]，安全攻击呈现出新特点，网络的安全性越来越受到重视[2-4]。由于计算机系统和信息网络系统本身固有的脆弱性[5]，越来越多的网络安全问题开始困扰着我们，黑客入侵和病毒蔓延的趋势有增无减，社会、企业和个人也因此蒙受了越来越大的损失。传统的安全保护类技术已经无法满足当前的需求。网络安全主动防御系统[6]是一种更深层次上进行的主动网络安全防御措施，它不仅可以通过监测网络实现对内部攻击、外部入侵和误操作的实时保护，有效弥补防火墙的不足，而且能够结合其他网络安全产品，对网络安全进行主动、实时的全方位保护。主动防御[7]是一种前摄性防御，由于一些防御措施的实施，使攻击者无法完成对目标的攻击，或者使系统能够在无需人为被动响应的情况下预防安全事件。主动防御将使网络安全防护进入一个全新的阶段，也被认为是未来网络安全防

* **收稿日期**：2017 年 10 月 8 日，**修回日期**：2017 年 11 月 26 日
作者简介：周亮，男，工程师，研究方向：计算机科学与技术。

护技术的发展方向。而主动防御的核心模块就是文件监控[8]，通过文件监控实时的监控系统可疑文件的操作，能够做到对病毒的防御。

针对上述问题，本文将介绍一种基于改进贝叶斯算法的文件监控系统。该系统实时监控所有的文件操作，并将可疑的文件行为进行分析评判。通过对传统的贝叶斯算法进行改进，提出一种基于加权的贝叶斯算法，在一定程度上弥补了传统贝叶斯算法在假设各特征向量无关联的偏差，提高了评判的准确性。

2　文件监控整体逻辑

本文提出的文件监控系统通过在驱动级捕捉文件的IO操作，并根据这个IO操作来判断这些文件的危险性。文件监控整体逻辑如图1所示，文件监控主要由驱动检测模块、行为分析模块以及查杀模块组成。驱动检测模块工作在驱动层，实时监控整个驱动层，并且捕捉文件的IO操作，经过过滤后把进入系统的可疑文件的行为信息以特征向量的形式上传到行为分析模块。行为分析模块工作在应用层，行为分析模块接收到驱动传递上来的行为特征向量之后，首先会与行为特征库进行比对，比对成功，把病毒信息返回给驱动；比对不成功则调用行为分析算法进行进一步分析，若判定为病毒，则把结果返回给驱动模块。驱动模块拿到分析的结果后，调用查杀模块对病毒文件进行隔离处理，本文侧重于介绍文件监控，对查杀模块不做介绍。

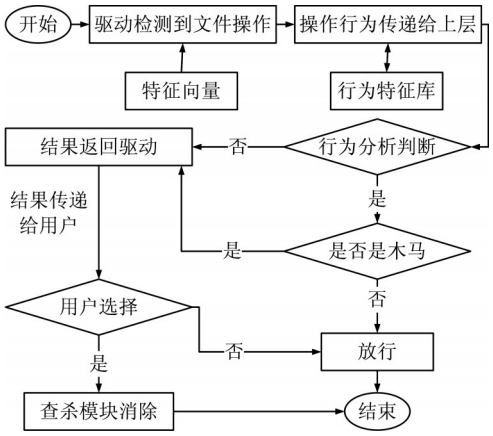

图1　文件监控整体流程

3　驱动检测模块

3.1　驱动检测模块阐述

病毒作为一种程序，想要在操作系统中获取用户信息，都必须调用操作系统提供的各种功能函数才能达到传播自身和破坏系统的目的[9]。而系统API对系统文件进行的读写操作，都会有IO操作传递到驱动模块[10]。因此驱动检测模块就利用病毒调用系统API的一系列行为提取出特征。同时，驱动会把正常的文件操作过滤掉，把可疑的或者无法确定的文件行为以特征向量的形式上传给行为分析模块，由该模块作进一步确定。

3.2　驱动过滤原理

Windows所有驱动程序都是IRP包驱动的[11]。IRP的全名是I/O Request Package，即输入输出请求包，它是Windows内核中的一种非常重要的数据结构。上层应用程序与底层驱动程序通信时，应用程序会发出I/O请求，操作系统将相应的I/O请求转换成相应的IRP，不同的IRP会根据类型被分派到不同的派遣例程中进行处理。病毒进行攻击时，调用系统API进行的文件操作都会是对系统文件的读写，而这些读写都会存放在IRP中，并下发到底层驱动。驱动检测模块可以对下发IRP包进行监听和拦截，然后对这些信息按照定好的规则进行分析，把不符合规则的文件信息上传到分析模块。

4　基于加权的改进贝叶斯算法

行为分析模块的主要作用是接受驱动模块传递上来的行为特征向量，并对这些行为特征向量进行分析，以便进一步确定文件是否是病毒文件。而分析的核心算法就是改进的基于加权的贝叶斯算法。

4.1　朴素贝叶斯算法

朴素贝叶斯算法[12]是一种分类算法（结构模型如图2所示），分类效果好、性能稳定、结构简单易于实现、计算效率高，而且算法的时间复杂度和空间复杂度都比较小，因此适合于检测未知的恶意程序，包括病毒。朴素贝叶斯分类用于木马行为分析时，分类集包括：木马程序、正常程序、不确定程序。待检测程序的一组异常行为特征组成的特征向量，且每个分量都是行为特征库中的行为特征。

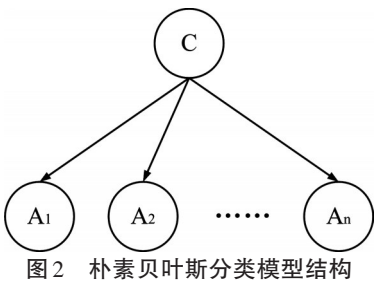

图2　朴素贝叶斯分类模型结构

朴素贝叶斯算法的基础，贝叶斯定理：

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

由贝叶斯定理可以看出,朴素贝叶斯[13]的思想是对给出的待分类项,求解在此项出现的条件下各个类别出现的概率,其中最大的概率所属类别即认为是待求分类项的类别。

朴素贝叶斯分类器的工作原理如下:

1)设 $X=\{a_1, a_2, \ldots, a_m\}$ 为一个待分类项,而每个 a 为 X 的一个特征属性。

2)有类别集合 $C=\{y_1, y_2, \ldots, y_n\}$。

3)统计得到在各类别下各个特征属性的条件概率估计。即:

$$\begin{cases} P(a_1|y_1), P(a_2|y_1), \cdots, P(a_m|y_1) \\ P(a_1|y_2), P(a_2|y_2), \cdots, P(a_m|y_2) \\ \cdots \\ P(a_1|y_n), P(a_2|y_n), \cdots, P(a_m|y_n) \end{cases} \quad (2)$$

假设各个特征属性是条件独立的,则根据贝叶斯定理有如下推导:

$$P(y_i|X)=\frac{P(X|y_i)}{P(X)} \quad (3)$$

由于 $P(X)$ 对所有类别都是相同的,可看作常数,因此只需计算分子即可:

$$P(X|y_i)P(y_i)=P(a_1|y_i)P(a_2|y_i)\cdots P(a_m|y_i)P(y_i)$$
$$=P(y_i)\prod_{j=1}^{m}P(a_j|y_i) \quad (4)$$

4)计算 $P(y_1|X), \ldots, P(y_n|X)$

5)计算 $P(y_k|X)=\max_{1\le i\le n}\{P(y_i|X)\}$

因此,$P(y_k|X)$ 最大值中的 y_k 即我们所求的分类。根据上述分析,朴素贝叶斯分类的流程可以由图3表示。

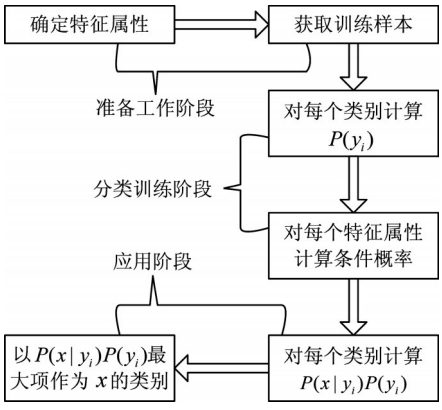

图3　朴素贝叶斯分类流程

由以上流程可知,整个朴素贝叶斯分类分为三个阶段:

第一阶段:准备工作阶段,这个阶段的任务是为朴素贝叶斯分类做必要的准备,主要工作是根据具体情况确定特征属性,并对每个特征属性进行适当划分,然后由人工对一部分待分类项进行分类,形成训练样本集合。这一阶段的输入是所有待分类数据,输出是特征属性和训练样本。这一阶段是整个朴素贝叶斯分类中唯一需要人工完成的阶段,其质量对整个过程将有重要影响,分类器的质量很大程度上由特征属性、特征属性划分及训练样本质量决定。

第二阶段:分类器训练阶段,这个阶段的任务就是生成分类器,主要工作是计算每个类别在训练样本中的出现频率及每个特征属性划分对每个类别的条件概率估计,并记录结果。其输入是特征属性和训练样本,输出是分类器。这一阶段是机械性阶段,根据前面讨论的公式可以由程序自动计算完成。

第三阶段:应用阶段。这个阶段的任务是使用分类器对待分类项进行分类,其输入是分类器和待分类项,输出是待分类项与类别的映射关系。这一阶段也是机械性阶段,由程序完成。

4.2　改进的贝叶斯算法

朴素贝叶斯模型发源于古典数学理论,因此有着坚实的数学基础,以及稳定的分类效率,其算法简单,对于小规模的数据表现很好,能够处理多分类任务,适合增量式训练。朴素贝叶斯算法是通过计算一些先验概率和特征的条件概率得出待验证的特征概率,这些先验概率是需要已有的样本集计算的,而有一个可靠的样本集至关重要。同时朴素贝叶斯算法在计算过程中是假设各特征属性之间是没有关联的,但是一个病毒的各种行为往往是相互影响的,因此该算法在某种程度上是有误差的,因此本文提出对该算法的一种改进。

综上所述,目前朴素贝叶斯算法存在两个问题:先验概率和特征的条件概率的计算以及特征属性之间的关联。先验概率和特征的条件概率的计算主要依赖于提供的样本集,而目前还没有公认的比较权威的木马样本集,因此主要依赖于研究者自己提供,为确保结果的可靠性,选择样本时尽量做到平均,把样本分为三类(木马程序、正常程序和不确定程序)。借鉴特征加权这一思想,提出基于特征加权的贝叶斯行为分析算法。

该算法的意思就是为程序的每个特征定义一个权值系数,该权值系数的含义是某一个特征行为对一个文件是否是病毒的影响程度。例如:正常程序和病毒修改注册表这一行为的目的显然是不一样的,病毒的行为更具危害,因此它的这一特征权值系数就比正常程序大。在实际应用中,不论是正常程序还是病毒程序,它们运行时的一系列行为是

相互关联的，而朴素贝叶斯的思想是假设这些行为特征没有关联，为修正这个假设带来的偏差，提出加权的思想。根据权值系数[14]的概念，为每一个程序的每一个类别增加一个加权系数，分别为：$\{w_1, w_2, \cdots, w_n\}$，用以调整后验概率的计算偏差。这些权值的大小由该特征对某一类别是不是病毒的影响程序来决定。在本文中，这些权值的具体数值由综合实验得出，并在之后的样本实验中根据错误分类进行调整。

根据以上分析，在朴素贝叶斯基础之上，为每个类别增加一个权值系数，最后计算公式为

$$P(y_i|X)=\frac{P(y_i)\prod_{j=1}^{m}P(a_j|y_i)}{P(X)} \tag{5}$$

$$P(y_k|X)=\max_{1\le i\le n}\{P(y_i|X)\} \tag{6}$$

因此，y_k 即我们所求的分类。其结构模型如图4所示。

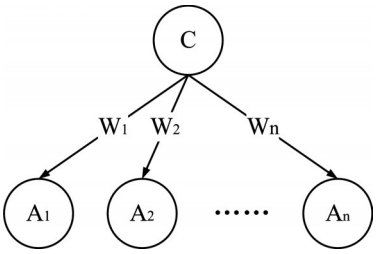

图4　基于特征加权的贝叶斯分类模型结构

4.3　详细算法流程

搜集大量的程序构成样本空间，根据上述将样本空间分成三类，即 $C=$｛病毒程序，正常程序，不确定程序｝。假设训练样本中收集的程序中有 a 个木马程序，b 个正常程序和 c 个不确定程序。则三个类别的先验概率分别为

$$\begin{cases}P(C_1)=\dfrac{a}{(a+b+c)}\\ P(C_2)=\dfrac{b}{(a+b+c)}\\ P(C_3)=\dfrac{b}{(a+b+c)}\end{cases} \tag{7}$$

然后从三种分类的程序中提取出行为特征 $X=\{a_1, a_2, \ldots, a_m\}$，例如：修改注册表 SHSetValueA、创建文件 CreateFileA、程序执行 CreateProcess 等调用系统 API 的行为。而对于某个行为特征，如 a_k，经过统计 a 个木马中表现此特征的个数是 d，b 个正常程序表现此特征的个数是 e，c 个正常程序表现此特征的个数是 f，则该特征在三个类别下的条件概率分别为

$$\begin{cases}P(a_k|C_1)=\dfrac{d}{a}\\ P(a_k|C_2)=\dfrac{e}{b}\\ P(a_k|C_3)=\dfrac{f}{c}\end{cases} \tag{8}$$

根据以上计算可以得到样本行为库。而对于一个待验证程 S，它的行为特征表示为 $X=\{a_1, a_2, \ldots, a_m\}$，对应三个类别的加权系数为 $W=\{w_1, w_2, w_3\}$。则对应的每个类别的概率为

$$\begin{cases}P(X|C_1)P(C_1)=P(C_1)\prod_{j=1}^{m}w_1P(a_j|C_1)\\ P(X|C_2)P(C_2)=P(C_2)\prod_{j=1}^{m}w_2P(a_j|C_2)\\ P(X|C_3)P(C_3)=P(C_3)\prod_{j=1}^{m}w_3P(a_j|C_3)\end{cases} \tag{9}$$

则该待验证程序的类别为上述三个最大值中的 C_i。

5　实验结果

通过搜集大量的程序构成样本空间。分为木马程序、正常程序以及不确定程序。样本数据如表1所示。每个类别选取200个构成最初的行为库，然后每个类别选择50个测试样本，计算错误率。

表1　实验的样本数据

样本分类	样本空间	训练集	测试集
木马程序	250	200	50
正常程序	250	200	50
不确定程序	250	200	50
总计	750	600	150

计算错误率中主要计算两类：1)将木马程序判断为正常程序，称为FN；2)将正常程序判断为木马程序，称为FP。从150条测试集中随机选择一些数据测试，测试结果如图5所示。

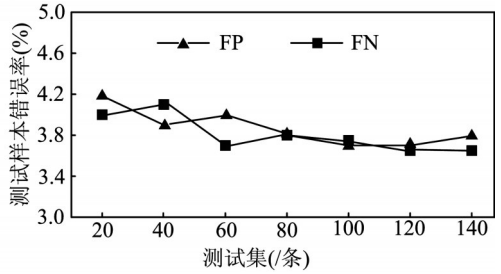

图5　测试样本错误率

从实验结果来看，排除一些人为造成的误差，在样本数量较少的情况下样本的错误率偏低，表明本文提出的文件监控在样本较少的情况下监控效

（下转第126页）

参 考 文 献

[1] 王晓杰. 电磁干扰的危害与防护[A]. 科技博览,2010(15):1-2.
[2] 刘尚合. 武器装备的电磁环境效应及其发展趋势[J]. 装备指挥技术学院学报,2005,16(1): 1-6.
[3] 关丹丹,侯莹莹. 电磁兼容仿真中的算法研究[J]. 电子质量,2009(6):68-70.
[4] GJB151B-2013. 军用设备和分系统电磁发射和敏感度要求与测量[S]. 2013:72-76.
[5] 陈晋吉. 飞行器电磁兼容预测仿真研究[D]. 西安:西安电子科技大学,2013:11-25.
[6] 房鸿瑞. 机载测控设备电磁兼容性设计与试验[C]//大型飞机关键技术高层论坛暨中国航空学会2007年学术年会论文集,2007:31-37.
[7] 赵翌池,宋祖勋,李恒博. 无人机机载通信设备间的射频电磁兼容预测分析[J]. 计算机与现代化,2012(6):5-8.
[8] 李明,朱中文,蔡伟勇. 电磁兼容技术研究现状与趋势[J]. 电子质量,2007(7):61-64.
[9] 关丹丹,侯莹莹. 电磁兼容仿真中的算法研究[J]. 电子质量,2009(6):68-70.
[10] 高建凯,周德俭. 三维布线技术的电磁兼容性预测[J]. 现代表面贴装资讯,2005,3(5):34-37.
[11] 周鹏辉,宋吉. 陀螺原理在航空仪表中的应用[J]. 黑龙江科技信息,2013(7):109-110.
[12] 洪瑞圭,李林和. 电子设备的电磁干扰及抑制分析[J]. 天津轻工业学院学报,2002(3):38-40.

(上接第85页)

果良好。在如今大数据时代,还需要更多的样本对该文件监控系统进行测试以确保其实际应用价值。

6 结语

本文为了实现文件监控的整体性,从驱动层拦截文件操作到上层的行为进行分析,到最终确定文件类别。本文重点介绍了行为改进的贝叶斯算法,在朴素贝叶斯算法模型的基础之上,提出基于特征加权的贝叶斯行为分析算法,该算法在一定程度上解决了朴素贝叶斯算法的一些缺点,如忽略特征属性之间的关联等。但该算法还是依赖于样本的训练,因此,如何确定样本的数量和质量也是研究的重点。经过实验分析,本文提出的文件监控效率良好,能够在信息安全等方面有良好的应用。

参 考 文 献

[1] 姜学东,王昊欣. 互联网网站网络安全威胁及策略分析[J]. 电子测试,2017(09):79-80.
[2] 龚俭,臧小东,苏琪,等. 网络安全态势感知综述[J]. 软件学报, 2017,28(04):1010-1026.
[3] 黄同庆,庄毅. 一种实时网络安全态势预测方法[J]. 小型微型计算机系统,2014,35(02):303-306.
[4] 赵颖,樊晓平,周芳芳,等. 网络安全数据可视化综述[J]. 计算机辅助设计与图形学学报,2014,26(05):687-697.
[5] 熊芳芳. 浅谈计算机网络安全问题及其对策[J]. 电子世界,2012(22):139-140.
[6] 董希泉,林利,张小军,等. 主动防御技术在通信网络安全保障工程中的应用研究[J]. 信息安全与技术, 2016,7(01):80-84.
[7] 张大伟,沈昌祥,刘吉强,等. 基于主动防御的网络安全基础设施可信技术保障体系[J]. 中国工程科学, 2016,18(06):58-61.
[8] 郝增帅,郭荣华,文伟平,等. 基于特征分析和行为监控的未知木马检测系统研究与实现[J]. 信息网络安全,2015(02):57-65.
[9] 曹玉林,马建萍. 基于微分方程的MANETs病毒传播模型研究[J]. 计算机工程. 2017(02):1-6.
[10] 吕晨,姜伟,虎嵩林. 一种基于新型图模型的API推荐系统[J]. 计算机学报,2015,38(11):2172-2187.
[11] 杨立敏,李耀华,王平,等. IRP理论和IEEE Std 1459-2010在变流器驱动电机能效测试中的应用比较[J]. 电工电能新技术, 2016,35(01):1-6,12.
[12] 皮靖,邵雄凯,肖雅夫. 基于朴素贝叶斯算法的主题爬虫的研究[J]. 计算机与数字工程,2012,40(06):76-78,123.
[13] 王辉,陈泓予,刘淑芬. 基于改进朴素贝叶斯算法的入侵检测系统[J]. 计算机科学,2014,41(04): 111-115,119.
[14] 毛明,杨谱,李旭飞. 递归扩散层的权值系数计算方法[J]. 计算机工程, 2014,40(11):126-129,134.