第 33 卷 第 7 期 计 算 机 工 程 2007 年 4 月
Vol.33 No.7 Computer Engineering April 2007
·安全技术· 文章编号：1000—3428(2007)07—0133—02 文献标识码：A 中图分类号：TP393.01

基于 *k*NN 算法的异常行为检测方法研究

卢 鋆，吴忠望，王 宇，卢 昱
(装备指挥技术学院研究生院，北京 101416)

摘 要：阐述了异常行为检测的相关概念，介绍了*k*NN算法，探讨了异常行为检测与分类技术的关系。结合*k*NN算法的优点以及异常行为检测与分类的相似性，提出了基于*k*NN算法的异常行为检测方法，给出了其计算方法，并确定了检测的过程，分析了该方法的特点和优势。基于*k*NN算法的异常行为检测方法通过不断的自学习，会成为信息安全的一道有效防线。

关键词：*k*NN 算法；分类；异常行为检测

Research on Abnormal Behavior Detection Based on *k*NN Algorithm

LU Jun, WU Zhongwang, WANG Yu, LU Yu
(Graduate School, Academy of Equipment Command and Technology, Beijing 101416)

【Abstract】 This paper elaborates the concepts related to abnormal behavior detection, introduces *k*NN algorithm and discusses the relationship between abnormal behavior detection and classification technologies. Based on the virtues of *k*NN algorithm and the comparability between abnormal behavior detection and classification, the method of abnormal behavior detection based on *k*NN algorithm is proposed and its calculation method and detection process is given. After analyzing its characteristics and advantages, it concludes that the method of abnormal behavior detection based on *k*NN will become an effective defense line of information security through continuous self-study.

【Key words】 *k*NN algorithm; Classification; Abnormal behavior detection

近年来，网络逐步应用到政府、军队、金融等各个领域，计算机网络已经成为国家的关键基础设施。随着网络的不断发展，网络安全问题日益严重，针对网络的各种攻击方式层出不穷，安全事件频频发生，不仅给企业、机构以及用户带来巨大的经济损失，而且也使国家的安全与主权面临严重威胁。入侵检测[1]技术的研究已经成为信息安全领域的热门课题。20 世纪 90 年代以来，基于统计学习原理[2]的文本分类[3]技术，如 *k*NN [4]（*k* Nearest Neighbor）算法，由于其出色的应用效果和发展潜力，目前正逐渐成为研究的热点和趋势，而在入侵检测过程中运用文本分类方法进行攻击行为的分析和判定也是一种新兴的研究方法。

1 异常行为检测的相关概念

入侵检测技术是一种主动发现网络隐患的安全技术，该技术能够帮助系统对付网络攻击，扩展系统管理员的安全管理能力，从而提高信息安全基础结构的完整性，是动态安全技术的核心技术之一。根据入侵检测所采用的分析技术可以分为异常[5]行为检测和误用检测。异常行为检测也称作基于行为[6]的（Behavior-Based）检测，它的基本前提是假定所有的入侵行为都是异常的，即入侵行为是异常行为的子集。首先需要建立系统或用户的正常行为特征轮廓（Profile），通过比较当前的系统或用户的行为是否偏离正常的行为特征轮廓来判断是否发生了入侵行为。该方法与误用检测不同，它不是依赖于具体行为是否出现来进行检测的，因此，异常行为检测对于检测未知的入侵行为非常有效，同时它也是检测冒充合法用户的入侵行为的有效方法。

2 基于 *k*NN 算法的异常行为检测

2.1 *k*NN 算法

*k*NN 算法又称作 *k* 最近邻算法，是一种统计学习方法，其实质是利用统计概率原理，采用计算机自动学习的方法，通过对已知样本的自动学习，建立特征体系，并实现对未知样本的预测。对于给未知文档向量分类，*k*NN 算法是将训练集的文档向量按文档近邻排列，随后使用 *k* 个最近似的类别标签来预测输入文档的类别，该算法根据样本内容，将其分到若干预先定义好的类中。文档邻居的确定可以根据欧几里德距离公式或者文档间向量的余弦测量得到，主要计算是对测试文档在训练文档集中评分，从而找到 *k* 近邻。

与 *k*NN 相似的文本自动分类算法有很多，包括朴素贝叶斯（Naïve Bayes）算法、神经网络算法、决策树算法以及支持向量机（Support Vector Machine，SVM）等。其中，*k*NN 算法作为非参数的分类算法，是非常有效和容易实现的，目前已经广泛应用于分类、回归和模式识别等。

2.2 异常行为检测与分类的关系

从数学角度来看，异常行为检测也是对被检测的未知行为进行分类的过程，未知行为与已知的正常行为相似，则该行为是正常行为，否则是入侵行为。把行为检测看作是一个映射的过程，其任务是将未标明类别的行为映射到已有的类别中，用数学公式表示如下：$f:A\rightarrow B$，其中，A 为待分类的行为集合，B 为分类体系中的类别集合。行为分类的映射规则是根据系统已经掌握的每类若干行为样本的数据信息，总结出分类的规律性而建立的判别公式和判别规则。然后在遇到新行为时，根据总结出的判别规则，确定行为相关的类别。

在异常行为检测中，漏报和误报都不能很好地判定入侵行为的发生。每天都有新的攻击方法产生，类型库和特征库

基金项目：国家“863”计划基金资助项目（2005AA149010）
作者简介：卢 鋆(1978－)，女，博士生，主研方向：网络控制和网络安全；吴忠望，硕士、助教；王 宇，副教授；卢 昱，教授、博导
收稿日期：2006-04-06 **E-mail：**junjun_lu@sina.com

得不到及时更新，就会造成漏报，入侵者成功进入，而入侵检测系统却没有告警。误报是指在没有明确的攻击事件时，入侵检测系统却不断地发出告警信息，过多的误报会导致安全日志迅速增长，不仅占去了大量存储空间，也加重了管理员的分析工作量。为了更好地评价异常行为检测方法的优劣，按照分类技术的评价标准，提出两个指标，即系统的微平均查准率P_{micro}和系统的微平均查全率R_{micro}。

系统的微平均查准率P_{micro}：

$$P_{micro}=\frac{\sum_{i=1}^{N}A_i}{\sum_{i=1}^{N}A_i+\sum_{i=1}^{N}B_i}$$

系统的微平均查全率 R_{micro} ：

$$R_{micro}=\frac{\sum_{i=1}^{N}A_i}{\sum_{i=1}^{N}A_i+\sum_{i=1}^{N}C_i}$$

其中，N 是系统的类别总数，A_i是正确分配到 i 类中的测试数，B_i是错误分配到 i 类中的测试数，C_i是属于但未分配到 i 类中的测试数。

2.3 基于 *k*NN 算法的异常行为检测

*k*NN 分类方法是建立在一定的假设之上的，即实例的分类与向量空间附近的其它实例的分类最近似，与其它文本分类法，如贝叶斯分类方法相比较，*k*NN 并不依赖于前期的概率，而且计算比较有效，主要的计算量是训练文本分类，用以发现测试文件的 *k* 最近邻，*k* 是个小常数。通过对进程的研究发现，系统调用的发生可以用来刻画程序行为的特征，将每个进程转换成一个向量，假设属于同一个类的进程会聚到一个向量空间。因此，可以把一个系统调用与系统调用序列的关系看作是字符与文本文件的关系，对系统调用的研究采用文本分类法。

在基于 *k*NN 算法的异常行为检测方法中，首先需要选择大的训练数据集，目的是保证所有可能的正常程序行为都包含在内，确保异常行为检测的准确性。其次是将程序行为序列转换成适合于学习算法和分类任务的表示形式，最常见的表示形式是向量空间模型（Vector Space Model，VSM）。在 VSM 模型中，每个进程都可以表示成系统调用向量，用矩阵 A 来表示进程集，每项代表系统调用在进程中出现，例如，$A=(a_{ij})$，a_{ij}是系统调用 i 在进程 j 中的权重。举例说明系统调用的短序列：*…open read write execve write open close…*，如果窗口尺寸为 3，则序列唯一。

open read write
read write execve
write execve write
execve write open
write open close

把系统调用序列转化为一个向量，如*…open read write write open close…*中*…open*的数目为 2，*read*的数目为 1，*write* 的数目为 2，*execve*的数目为 1，*close*的数目为 1。用f_{ij}表示系统调用i在进程j中出现的频率，N代表集合中进程的数量，M代表在集合中不同系统调用的数量，对于矩阵A来说，行的数量与M的值相同。用n_i代表系统调用i在整个集合中出现的次数。确定权重a_{ij}的方式有多种，最简单的方法是布尔加权法，当系统调用在程序中出现时，a_{ij}等于 1，否则为零，还可以使用系统调用在程序中出现的频率来确定，如$a_{ij}=f_{ij}$。另外，还可以使用TF-IDF（Term Frequency-Inverse Document Frequency）法来确定，这种方法更常用，在这种加权方法中，$a_{ij}=f_{ij}\times\log(\frac{N}{n_i})$，同时，考虑进程的长度不同，对TF-IDF 方法也可以稍微做些改变，得到：

$$a_{ij}=\frac{f_{ij}}{\sqrt{\sum_{i=1}^{M}f_{ij}^2}}\times\log(\frac{N}{n_i})$$

对于进程 X 而言，*k*NN 算法能够将训练集中进程的邻居进行排列，使用 *k* 大多数相似的邻居的分类标签来预测新进程的类。这些邻居的类的权值使用每个邻居和 X 的相似性来定，相似性由两个进程向量的欧几里德距离或余弦值确定，定义如下：

$$sim(X,D_j)=\frac{\sum_{t_i\in(X\cap D_j)}x_i\times d_{ij}}{\|X\|_2\times\|D\|_2}$$

其中，X是测试进程，用向量表示；D_j是第j个测试进程，t_i是X和D_j共享的系统调用，x_i是系统调用t_i在X中的权重，d_{ij}是系统调用t_i在D_j中的权重，$\|X\|_2=\sqrt{x_1^2+x_2^2+x_3^2+...}$，是X的范数，$\|D_j\|_2$是$D_j$的范数。

基于 *k*NN 算法的整个异常行为检测过程如图 1 所示。

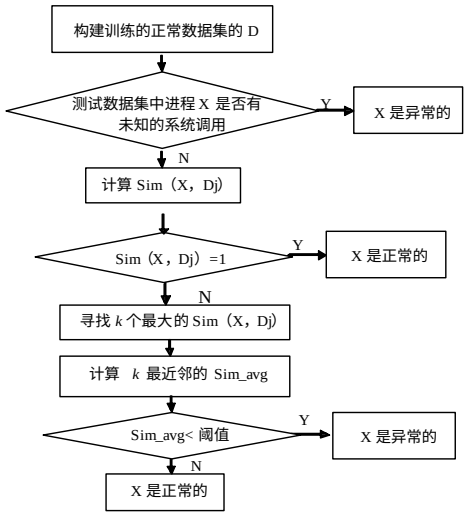

图 1 基于 *k*NN 算法的异常行为检测过程

除了对正常行为进行编码加入训练集，也可以对恶意行为进行编码，加入训练集。通过训练和测试，可以发现基于 *k*NN 的异常行为检测具有适用于动态环境和实时入侵检测的优点，能够有效地检查入侵程序行为，不需要单个的程序轮廓，主要凭借基于实例的不断自动学习来提高准确性，达到低的 false positive 率。当 *N* 比较大时，该方法对于某些实时入侵检测系统而言，计算量会比较大，为了提高攻击检测的有效性，*k*NN 异常检测方法还可以和攻击签名（误用）检测结合使用。

3 结束语

基于 *k*NN 的异常行为检测方法善于学习用户/系统或网络行为，提取使用模式和规则，识别新实例，通过学习经验自动改进，对于防止恶意代码、滥用和非法行为等非常有效。该方法是一种直推法，直接从已知进程集对特定的未知行为样本进行识别的方法，计算复杂度小。正是因为基于 *k*NN 的异常行为检测方法可以充分发挥计算能力，并且效果优于传统计算方法，所以具有很大的发展潜力，是网络防护和信息安全领域需要重视和引用的一项重要技术。（下转第 138 页）