基于核函数 Fisher 鉴别的异常入侵检测

周鸣争
(安徽工程科技学院计算机科学与工程系 芜湖 241000)

摘 要 将核函数方法引入入侵检测研究中，提出了一种基于核函数 Fisher 鉴别的异常入侵检测算法，用于监控进程的非正常行为。首先分析了核函数 Fisher 鉴别分类算法应用于入侵检测的可能性，然后具体描述了核函数 Fisher 鉴别算法在异构数据集下的推广，提出了基于核函数 Fisher 鉴别的异常入侵检测模型。并以 Sendmail 系统调用序列数据集为例，详细讨论了该模型的工作过程。最后将实验仿真结果与其它方法进行了比较，结果表明，该方法的检测效果优于同类的其它方法。

关键词 异常入侵检测，核函数 Fisher 鉴别，异构数据集，系统调用
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2006)09-1727-04

An Anomaly Intrusion Detection Based on Kernel Fisher Discriminant

Zhou Ming-zheng
(*Dept. of Comp. Sci. & Engn., Anhui University of Technology and Science, Wuhu* 241000, *China*)

Abstract Kernel method is introduced to intrusion detection and an anomaly intrusion detection method based on kernel Fisher discriminant is presented in this paper. This method is applied for monitoring the abnormal behavior of processes. Firstly, this paper presents the possible of kernel Fisher method applied to intrusion detection. Secondly, this paper descriptions the kernel Fisher algorithm is generalized for heterogeneous datasets. A model of anomaly intrusion detection based on kernel Fisher is given and the working process of this model is used with sendmail system call in detail discussion; Finally, the simulation result is compared with other methods, The measuring result of this method is superior to other similar methods .

Key words Anomaly intrusion detection, Kernel Fisher discriminant, Heterogeneous datasets, System call

1 引言

入侵是指破坏资源保密性、完整性和可用性的一组行为，入侵检测则是网络安全深层防卫系统的重要组成部分，通过监测和分析网络流量、系统审计记录等，发现和识别系统中的入侵行为和入侵企图，给出入侵报警，以便系统管理员采取有效的措施弥补系统漏洞和填补系统功能，目前针对它的研究是一个热点。

入侵检测方法一般可分为两大类：滥用入侵检测(misuse detection)和异常入侵检测(anomaly detection)。滥用入侵检测的基础是建立黑客攻击行为的特征库，采用特征匹配的方法确定攻击事件。其优点是检测误报率低，速度快，但通常不能发现攻击特征库中没有的实现指定的攻击行为，所以也无法检测出新的攻击。异常检测是通过建立用户正常行为模型，以是否显著偏离正常模型为依据进行入侵检测。它有一定的误报率，但它可根据当前的系统行为用正常模型的相似度判断是否为攻击，有可能发现新的攻击行为。这两种方法都需要对用户行为进行建模，滥用检测需要建立攻击行为模式；异常检测需要建立正常用户的行为模式。基于机器学习的用户行为建模始终是入侵检测系统(Intrusion Detection System，IDS)的一个重要研究课题。以往的研究者在IDS研究中引入了各种机器的学习方法，如神经网络[1]，遗传算法[2]，HMM[3]，模糊综合评判[4]等，但这些方法多是基于样本数目趋于无穷大假设的。并且对数据的规律性要求较高，在IDS中能够获得的数据往往呈现出多变性、小样本和高维性，较难满足上述这些算法的要求，使得检测结果实用性较差，误报率较高。

近几年来成为机器学习研究热点的核函数方法，是一种比较完备的从小样本数据中寻找规律的系统方法，主要用于解决有限样本的模式识别分类问题。本文将核函数 Fisher 鉴别应用于入侵检测中，针对 IDS 中经常出现的异构数据集情况，构造了基于异构距离定义的 RBF 形核函数，提出了一种异构数据集下的核函数 Fisher 异常鉴别的网络入侵检测方法，以保证在先验知识不足的情况下，系统仍有较好的分类正确率，从而使得整个 IDS 具有较好的检测性能。

本文首先讨论了核函数 Fisher 鉴别应用于 IDS 的可行性，然后具体描述了核函数 Fisher 鉴别算法在异构数据集下的推广，并提出基于核函数 Fisher 鉴别的异常入侵检测系统的模型，最后以网络连接记录集作为入侵检测数据，详细讨论了该模型的工作过程和实验仿真结果。

2005-01-10 收到, 2005-06-21 改回
安徽省教育厅自然科学重点基金(2004kj033zd)资助课题

2 核函数 Fisher 鉴别与入侵检测

2.1 核函数 Fisher 鉴别应用于入侵检测的可行性

从方法上讲，滥用入侵检测的核心是攻击行为模式的正确表达和快速识别。异常入侵检测的核心是用户正常行为模式的建立以及正常模式和异常模式的识别和分类，这些都是典型的模式识别问题。因此广义上讲入侵检测是属于模式识别的范畴。从本质上讲，入侵检测可以看作是一个分类问题，也就是通过检测把正常数据与异常数据分开，但是 IDS 中需要分类的数据更加复杂，常常体现为高维、小样本和不可分性。基于 Fisher 鉴别是一种建立在统计学习理论基础之上的分类方法，可广泛用于小样本数据，而且对数据维数不敏感，即由有限的训练集样本得到小的误差仍然能够保证对独立的测试集保持小的误差。同时也可用于密度估计和孤立点的发现，既不均衡数据集中无监督的异常检测问题。因此基于核函数 Fisher 鉴别适合于入侵检测中对高维异构不均衡数据集进行分类和异常发现，将其应用于入侵检测是可行的。

2.2 核函数 Fisher 鉴别算法

2.2.1 线性Fisher鉴别　在模式识别中，Fisher提出的多测量统一归一化思想为各类Fisher鉴别奠定了基础。线性Fisher鉴别[5]是从d维输入空间得到一维输出空间的数学变换方法。设X包含N个d维样本，其中N_i个样本属于类别W_i，x_i^j表示类别j的第i个样本；若对$x_i\in R^d$的分量作线性组合可得标量：

$$y_i = w^{\mathrm{T}} x_i, \quad i = 1,\cdots,N \tag{1}$$

该式表明每个y_i为对应的x_i到方向为w的直线上的投影，w的方向不同，将使样本投影后的可分离程度不同，从而直接影响识别效果。线性Fisher鉴别函数定义为

$$\boldsymbol{J}(\boldsymbol{w}) = \frac{w^{\mathrm{T}}\boldsymbol{S}_b w}{w^{\mathrm{T}}\boldsymbol{S}_w w} \tag{2}$$

其中

$$\boldsymbol{S}_w = \sum_{j=1}^{2}\sum_{i=1}^{N_j}(x_i^j - \boldsymbol{m}_j)(x_i^j - \boldsymbol{m}_j)^{\mathrm{T}} \tag{3}$$

$$\boldsymbol{S}_b = (m_1 - m_2)(m_1 - m_2)^{\mathrm{T}} \tag{4}$$

$$\boldsymbol{m}_j = \frac{1}{N_j}\sum_{i=1}^{N_j} x_i^j, \quad j = 1,2 \tag{5}$$

$\boldsymbol{S}_w$称为类内散布矩阵，$\boldsymbol{S}_b$称为类间散布矩阵，$\boldsymbol{m}_j$为类别j的均值向量，使(2)式取极大值时的W^*即为所寻找的最佳投影方向，即

$$\boldsymbol{w}^* = s_w^{-1}(m_1 - m_2) \tag{6}$$

将式(6)代入式(1)，即可将d维样本投影为一维，从而实现多维空间到一维空间的映射，任意一个测试样本x到方向为W^*的投影为$G(x)=W^{*\mathrm{T}}x$，其决策函数:

$$\boldsymbol{F}(\boldsymbol{x}) = \mathrm{sgn}(G(x) + b_0) \tag{7}$$

其中b_0为决策阈值。

2.2.2 用于孤立点发现的核函数Fisher鉴别　线性Fisher判别虽然能够找到一条较好的易于分类的投影线，但在实际情况下，线性方法非常有限，常常不能有效地解决非线性问题，现在将输入空间的样本数据$x\in R^d$经过非线性映射 Φ变换到特征空间F中，即

$$\phi: R^d \to F, x \to x' \tag{8}$$

其中 $x' = \phi(x)$， $x' \in F$ ，这样在特征空间F中，可利用线性Fisher鉴别。首先引入核函数$k(x_i, x_j)$，权值向量$\boldsymbol{w}$在特征空间F中可以按所有训练样本数据展开，即

$$\boldsymbol{w} = \sum_{k=1}^{N} a_k\phi(x_k) = \sum_{k=1}^{N} a_k k(x_i, x_k) \tag{9}$$

这样对于输入空间的样本数据而言，其核函数 Fisher 鉴别函数为

$$\boldsymbol{J}(\boldsymbol{a}) = \frac{a^{\mathrm{T}}P^a}{a^{\mathrm{T}}Q_a} \tag{10}$$

其中

$$\boldsymbol{P} = (P_1 - P_2)(P_1 - P_2)^{\mathrm{T}} \tag{11}$$

$$p_j = (p_{jk}), \quad j = 1,2, \quad k = 1,\cdots,N \tag{12}$$

$$p_{jk} = \frac{1}{N_j}\sum_{i=1}^{N_j} k(x_k x_i^j), \quad j = 1,2, \quad k = 1,\cdots,N \tag{13}$$

$$Q = \sum_{j=1}^{2}\sum_{i=1}^{N_j}(\boldsymbol{k}_i^j - p_j)(\boldsymbol{k}_i^j - p_j)^{\mathrm{T}} \tag{14}$$

$\boldsymbol{k}_i^j$表示第j类别，大小为$N\times1$ 维核矩阵，每个元素大小等于$K(x_k, x_i^j)$， $k = 1,\cdots,N$ 。式(10)的极值求解方法类似于线性Fisher鉴别方法，其解为

$$a = Q^{-1}(p_1 - p_2) \tag{15}$$

任意一个测试样本 x 到方向为 $\boldsymbol{w}$ 的投影为

$$G(x) = (\boldsymbol{w}\phi(x)) = \sum_{i=1}^{N} a_i k(x_i, x) \tag{16}$$

其判别函数为

$$F(x) = \mathrm{sgn}(G(x) + b_0) \tag{17}$$

其中b_0为决策阈值。这样就通过核函数将输入空间转化到特征空间中，然后在特征空间中构造超平面，根据数据到原点的距离来实现分类，发现孤立点。

2.3 基于核函数 Fisher 的入侵检测系统

2.3.1 异构数据集上的核函数 Fisher 鉴别　传统的核函数 Fisher 鉴别是在输入空间为内积空间下推导出来的，而异构数据集上通常无法定义内积。为此在文献[6]的基础上，提出了一种基于异构数据集上的异构距离的核函数，将核函数 Fisher 在异构数据集上进行了推广。

设$x, y\in X,$ 则x, y之间的异构距离可用以下方式定义[6]

$$H(x,y) = \sqrt{\sum_{a=1}^{m} d_a^2(x_a, y_a)} \tag{18}$$

其中

$$d_a(x,y)=\begin{cases}1, & \text{如果}x_a\text{或}y_a\text{未知}\\ \text{normalized}-\text{vdm}_a(x,y), & \text{如果第}a\text{个属性}\\ & \text{是离散值}\\ \text{normalized}-\text{diffa}_a(x,y), & \text{如果第}a\text{个属性}\\ & \text{是连续值}\end{cases} \tag{19}$$

$$\text{normalized}-\text{diffa}_a(x,y)=\frac{|x-y|}{4\sigma_l} \tag{20}$$

$$\text{normalized}-\text{vdm}_a(x,y)=\sqrt{\sum_{c=1}^{C}\left|\frac{N_{a,x,c}}{N_{a,x}}-\frac{N_{a,y,c}}{N_{a,y}}\right|^2} \tag{21}$$

g为数据集上第l个属性的方差，$N_{a,x}$为数据集X上所有数据第a个属性取值为x_a的数据个数，$N_{a,x,c}$为数据集X上的所有数据第a个属性取值为x_a，且输出类别为C的数据的个数，C是数据集的所有输出类别。

这种距离定义对不同的属性采用不同的距离定义方式，最终的距离用各个属性分量的欧氏距离来获得，充分表达了数据集之间的相似性，更好度量数据之间的距离而且计算比较简单、高效。

通常入侵检测中使用的数据集为一异构数据形，这就需要构造一个特殊的核函数将这种向量数据集变换到一个内积空间上，然后实现各种算法。我们对 RBF 核函数进行了改进来完成这种变换，用输入异构数据集上的异构距离来代替范数，再通过 RBF 核函数定义将输入数据集映射到一个特征空间，构成一个满足 Fisher 鉴别的条件，用这种改进的 RBF 核函数做 Fisher 鉴别分类。最终的核函数定义为

$$K(x,x_i)=\exp(-H(x,x_i)/\delta^2) \tag{22}$$

其中 H 为异构距离函数。

2.3.2 基于核函数 Fisher 的入侵检测　基于核函数 Fisher 的入侵检测系统主要由审计数据预处理器，核函数 Fisher 分类器两部分组成，如图 1 所示：

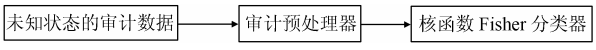

图 1　基于核函数 Fisher 的入侵检测系统

审计数据预处理系统用于对大量的系统审计记录进行处理和变换，由于其核函数 Fisher 的分类器只能对维数相同的数字向量进行分类，但有时系统审计数据中的数据不但长度不尽相同，而且很有可能不是数字类型，所以必须将审计数据按距离函数的定义转换成核函数 Fisher 分类器能够处理的数字向量；核函数分类器对这些数字向量进行分类，产生分类结果，这些结果可以直接作为整个入侵检测系统的输出。

系统工作分为训练阶段和检测阶段，在训练阶段，根据已知的正常审计数据和异常审计数据按式(10)训练基于核函数的 Fisher 函数，并根据式(9)和式(15)得到相关的参数；在检测阶段，预处理器先将未知状态的审计数据处理成数字向量的形式，然后通过核函数 Fisher 鉴别分类器，根据式(17)对输入数字向量进行分类，并将分类结果提交给决策系统作出最后的判断。

3　实验测试及分析

为便于比较，本文方法测试采用美国新墨西哥大学计算机科学系 Stephanie Forrest 教授领导的实验室收集的系统调用序列数据集 Sendmail。系统调用序列是入侵检测中使用比较普遍的一种审计数据，一条系统调用序列就是一个进程在运行过程中发出的所有系统调用的顺序序列，在这个序列可以通过系统中的应用程序(比如 strace)获得。一个正常行为可以由其执行迹局部模式，即系统调用短序列来描述其程序执行代码具有相对的稳定性。在异常行为中，可能出现和正常情况有一定差别的系统调用短序列。所以，某个进程发出的执行迹是正常的还是异常的就转化为识别执行迹中的短序列是正常的还是异常的，进而确定该进程是否有安全方面的问题。

3.1　实验数据的预处理

Sendmail进程常用在Unix系统下，完成接收和发送邮件工作，是一个重要的进程，每个系列数据文件有两列整数组成，第 1 列表明进程ID号，另一列则是代表某个系统调用号。这些代号可以通过一个索引文件转化成具体的系统调用名称，例如：代号“5”表示名称为“Open”的系统调用进程标识符相同的系统调用构成一个进程的执行迹。Sendmail进程可以分叉，它的子进程产生的系统调用序列被单独跟踪，但它们也被包括在当前Sendmail的序列中，用不同的PID加以区分，由于其审计数据已是数字序列，预处理的主要目的是得到该执行迹的系统调用短序列。实验时先对原始序列切割成某一给定长度的序列段；根据Lee[7]从信息论的角度研究的选择结果，认为最适合的系统调用短序列长度为 6~7。本实验中，数据预处理采用长度为 6 的窗口在程序执行迹上滑动来得到执行迹的短序列，通过对正常的系统调用执行迹扫描，可以得到正常的系统调用短序列样本。对异常的执行迹扫描时，会得到一组既有正常短序列又有异常短序列的系统调用短序列列表，通过比较，就构成了异常短序列样本，然后随机抽取 10%作为训练集，剩余的 90%作为测试集。

3.2　实验结果及讨论

通过训练，得到核函数 Fisher 判别相关参数后，首先用长度为 6 的滑动窗口对测试集的执行迹进行扫描，产生一组系统调用短序列。将这些系统调用短序列作为基于核函数 Fisher 分类器的输入，利用式(9)可以得到相应执行迹的状态。表 1 为本文训练数据和检测数据的分配情况。表 2 为其本文方法的仿真结果以及与 Forrest 等在文献[8]中和 Lee 等在文献[9]中得出研究结果的比较，通过比较，可以看到，本文的方法具有一定的优势。从正常异常的差值(异常序列中的最小异常度减去正常序列的异常度)来看，Forrest 方法给出的结果是 5.66，Lee 的方法给出的结果是 24.27，而我们的方法得到的结果为 24.46。我们的方法略好于 Lee 的方法，但若同时

考虑正常序列异常度的实际值，我们的方法是 1.14 为 Lee 方法的 1/4，Forrest 将所有的正常序列用于训练，正常序列的异常度必然为 0，不能说明其准确度高。基于上述的讨论，可以看出在 3 种方法中，本文方法对进程正常行为的表达更准确，能最有效地将正常和异常执行序列区分开来，在给定的误报水平上，可以降低阈值，减少漏报。同时，它不需要全部的正常和异常的信息，在给出较少的正常和异常执行迹的情况下就能得到比较理想的检测效果。由于入侵检测的问题实际训练数据的搜索一般比较困难，这个特性十分有利于实际系统的应用。

表 1 训练和检测数据的分配情况

	正常执行迹	异常执行迹
训练数据集	30	15
测试数据集	2603	987

表 2 3 种入侵检测方法的性能比较

	Forrest	Lee	本文方法
异常序列最大值	100	100	100
异常序列最小值	5.66	28.68	25.60
正常序列	0	4.41	1.14

4 结束语

通过理论分析和对 Sendmail 系统调用数据集的实验验证表明，本文提出的基于核函数 Fisher 鉴别的入侵检测方法，只需要较少的训练数据，就能得到较好的结果，具有较高的检测性能和较快的检测速度，如果将基于此模型的入侵检测算法用于实时检测，对系统性能的影响较小，是一种高效、低负荷的检测方法。

参 考 文 献

[1] Anup K Ghosh, Aaron Schwartzbard. A study in using neural networks for anomaly and misuse detection. The 8th USENIX Security Symposium, Washington D C, 1999: 46−57.

[2] Balajinath B, Raghavan S V. Intrusion detection through learning behavior model. *Computer Communications*, 2001, 24(12): 1202−1212.

[3] Jha S, Tan K, Maxion R A. Markov Chains, classifiers and intrusion detection. The 14th IEEE Computer Security Foundations Workshop, Canada, 2001: 206−215.

[4] 张箭, 龚俭. 一种基于模糊综合评判的入侵异常检测方法. 计算机研究与发展, 2003, 40(6): 776−782.

[5] Fisher R A. The statistical utilization of multiple measurements. *Annals of Eugenics*, 1938, 6(8): 376−386.

[6] Wilson D, Martinez R. Improved heterogeneous distance functions. *Journal of Artificial Intelligence Research*, 1997, 6(1): 1−34.

[7] Lee W, Stolfo SJ. A data mining framework for building intrusion detection medel, In: Gorgl, Keiter M K, eds. Proceedings of He 1999 IEEE Symposium on Security and Privacy, Oakland, CA, IEEE Computer Society Press, 1999: 120−132.

[8] Forrest S, Hofmeyr S A, *et al*.. A sense of self for unix process. In: Proceedings of 1996 IEEE Symposium on Computer Security and Privacy, Canada, 1996: 120−128.

[9] Lee W, Stolfo S, Chan P. Learning patterns from unix process execution traces for intrusion detection. In: Proceeding of AAAI Workshop: AI Approaches to Fraud Detection and Risk Management, Washington D C, 1997: 191−197.

周鸣争： 男，1958 年生，教授，主要研究领域为人工智能与网络安全.