Hans Journal of Data Mining 数据挖掘, 2014, 4, 27-31
Published Online October 2014 in Hans. http://www.hanspub.org/journal/hjdm
http://dx.doi.org/10.12677/hjdm.2014.44004

Hans汉斯

The SVM Intrusion Detection Problem Based on Nonlinear Projection and Penalty Function

Yuquan Cui, Linlin Li, Danxing Cao

The School of Mathematics, Shandong University, Jinan
Email: cuiyq@sdu.edu.cn

Received: Jul. 17th, 2014; revised: Aug. 21st, 2014; accepted: Sep. 3rd, 2014

Abstract

Based on the idea of a linear projection pursuit, we propose a method for nonlinear projection. The nonlinear projection method will reduce the high dimensional data into low-dimensional space. For low-dimensional data projection thus obtained with a penalty function reuse nonlinear support vector model and implement intrusion detection data. Finally, we use the KDD99 data set to illustrate the model's effectiveness. Verified by calculation, the effect is more ideal.

Keywords

Nonlinear Projection, Penalty Function, Support Vector Machine, Intrusion Detection

基于非线性投影和带惩罚函数的SVM的入侵检测问题

崔玉泉，李琳琳，曹丹星

山东大学数学学院，济南
Email: cuiyq@sdu.edu.cn

收稿日期：2014年7月17日；修回日期：2014年8月21日；录用日期：2014年9月3日

摘　要

本文根据线性投影寻踪的思想，提出了一种非线性投影方法。该方法通过非线性投影将高维数据降低到低维空间，对于由此投影得到的低维数据再利用带惩罚函数的非线性支持向量模型，实现对入侵数据的检测。最后，利用KDD99数据对本模型进行验证，以说明其有效性。经计算验证，效果较为理想。

关键词

非线性投影，罚函数，支持向量机，入侵检测

1. 引言

随着计算机网络技术的快速发展，网络安全问题成为人们非常关注的问题，网络攻击层出不穷，如物理攻击、数据攻击、密码盗取、拒绝服务等，传统的防御措施已难以抵御这些攻击，由此入侵检测问题成为了网络安全领域的一个重要研究分支。入侵检测方法是一种主动保护自己免受攻击的一种网络安全技术，它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，提高信息安全基础结构的完整性。它从网络系统中的若干关键点收集信息，并分析这些信息，因此常被认为是防火墙之后的第二道安全闸门。入侵检测方法[1] [2]主要分滥用(或误用)检测(Misuse Detection)和异常检测(Anomaly Detection)，其中异常检测是预先建立用户正常行为模型，根据系统状态是否偏离其正常状态进行检测，其偏离正常状态的即判定为入侵。为了得到理想的检测效果，人们已经进行的大量的研究与探索，如基于神经网络理论、贝叶斯理论、支持向量机理论[3]-[7]等理论方法的研究与应用，这些方法在入侵检测中，都取得了较好的效果。这些方法大都是从提高入侵检测率、降低虚警率等方面出发，未能较充分的考虑入侵方面的特征分析。而在高维数据[8]中，不相关特征或冗余特征可能会带来负面影响，对入侵检测率不仅不会提高，还会使其下降。因此，本文考虑利用非线性投影方法，将高维数据降低到低维数据，对于得到的低维数据再利用带惩罚函数的非线性支持向量模型，实现对入侵数据的检测。最后，利用 KDD99 数据对本模型进行验证，以说明其有效性。通过对数据的计算检验，模型的效果较为理想。

2. 非线性投影方法介绍

线性投影寻踪(Projection Pursuit)方法是用来分析和处理高维观测数据，特别是处理来自非正态总体的高位数据的一种统计方法，其基本思想是把高维数据线性投影到低维空间，寻找出能反映高维数据的结构或特征的投影。由于线性投影在将高维数据投影到低维空间时，可能会改变数据的结构或特征，因此本文考虑非线性投影方法，其方法如下：

设有 m 维的数据，其样本量为 n，用 m 维的数据的投影值构造的综合评价指标，记为 z，则有

$$Z_j = \sum_{i=1}^{m} a_i \Phi(x_i)$$

其中 a 是投影参数 $\left(a = (a_1, a_2, \cdots, a_m)^{\mathrm{T}}\right)$，$X$ 为 m 维向量，由 m 维数据向更高维空间的映射定义为：$\Phi : x_i \to \Phi(x_i)$。确定综合指标 z 的关键是找到反映高维数据结构特征的最优投影方向 a。由于投影方向可选取为单位向量，因此，优化投影方向可变为求解有约束的优化极值问题，即构造一个投影指标 $Q(a)$，建立如下模型：

$$\begin{cases}\min Q(a)\\ \|a\|=1\end{cases} \tag{1}$$

这里可考虑选取投影后的点 Z_i (其维数为一维)与 Z_j 的积与原数据集的点 X_i (其维数为 m 维)与 X_j 的点积的差的平方和最小作为目标，即：

$$Q(a)=\sum_{i=1}^{n}\sum_{j=1}^{n}\left(Z_iZ_j-X_i^{\mathrm{T}}X_j\right)^2+v\sum_{i=1}^{m}P(a_i) \tag{2}$$

其中 $Z_iZ_j=\sum_{l=1}^{m}\sum_{k=1}^{m}a_la_kK\left(x_{il},x_{jk}\right)$， $P(a_i)$ 为罚函数。当然更一般的模型可考虑

$$Q(a)=\left(\sum_{i=1}^{n}\sum_{j=1}^{n}\left(Z_iZ_j-X_i^{\mathrm{T}}X_j\right)^p\right)^{\frac{1}{P}}+v\sum_{i=1}^{m}P(a_i) \tag{3}$$

由此，可确定投影方向 a，从而将原高维数据降维。

3. 利用 SVM 方法进行检测

SVM 方法是 V. Vapnik 及合作者在统计学习理论基础上发展起来的学习算法，它通过结构风险最小化原则来最小化实际风险，具有泛化能力强，能处理高维小样本数据等特点，其主要思想是通过某种事先选择的非线性映射将输入向量映射到高维空间，在高维空间上构造最优分类超平面。SVM 的主要模型分为线性可分模型、线性不可分模型、非线性可分模型及非线性不可分模型，主要用于数据分类及回归分析等问题，具有罚函数的非线性不可分模型设计如下：

设样本集为 (x_i,y_i)，$i=1,2,\cdots,n,x\in R^d$，$y_i\in\{-1,+1\}$，SVM 方法是将输入数据映射到高维特征空间，并在此空间构建一个最优分离超平面。用 $\phi(x)=\left(\phi_1(x),\phi_2(x),\cdots,\phi_m(x)\right)$ 表示特征映射，则最优分离超平面为 $y(x)=\mathrm{sgn}\left(w\cdot\phi(x)+b\right)$，其中 w 为权向量， b 为常数。SVM 的非线性不可分二分类模型如下：

$$\min H(w,\xi)=\frac{1}{2}w^{\mathrm{T}}w+C\sum_{i=1}^{n}\xi_i+T\sum_{j=1}^{m}P_r\left(w_j\right)$$

$$s.t\begin{cases}y_i\left(w^{\mathrm{T}}\phi(x_i)+b\right)\geq 1-\xi_i & i=1,2,\cdots,n\\ \xi_i\geq 0\end{cases} \tag{4}$$

其中 C 是正则化参数，控制最小化误差和最大化边缘之间的折中； ξ_i 是松弛变量，度量不可分情况下样本违反约束的程度； $P_r(w_i)$ 为罚函数。

核函数 $K(x_i,x_j)$ 满足 Mercer 条件，即： $K(x,y)=\sum_{m=1}^{\infty}\alpha_m\phi(x)\phi(y)$， $\alpha_m\geq 0$

$$\iint K(x,y)g(x)g(y)\mathrm{d}_x\mathrm{d}_y\succ 0,\quad \int g^2(x)\mathrm{d}x\prec\infty \tag{5}$$

常用的核函数有以下几种：

1) 多项式核函数：$K(x,y)=\left((x\cdot y)+1\right)^d$ 或 $K(x,y)=(x\cdot y)^d$ (6)

2) 径向基核函数： $K(x,y)=\exp\left(-\frac{(x-y)^2}{2\sigma^2}\right)$ (7)

3) 扩展径向基函数： $K(x,y)=\exp\left(-\frac{|x-y|}{2\sigma^2}\right)$ (8)

4) Sigmoid 核函数： $K(x,y)=\tanh\left(v(x\cdot y)+c\right)$ (9)

罚函数 $P_r(w_i)$ 的形式，常见的有：

1) $L_1: P_r(\eta)=\gamma(\eta)$ (10)

2) $L_2: P_r(\eta)=\gamma(\eta)^2$ (11)

3) $L_p: P_r(\eta)=\gamma^2-(\eta-\gamma)^2 I(|\eta| \prec \gamma)$ (12)

4) $P_r(\eta)=\gamma I(\eta \le \gamma)+\frac{(a\gamma-\eta)}{a-1} I(\eta \succ \gamma)$ (13)

根据已有的网络入侵数据集，如 KDD99 数据集，首先利用非线性投影寻踪方法分别将数据的 41 维特征空间投影到低维空间中(如 4 维空间中)。而后，利用 SVM 的带罚函数的非线性不可分模型，按降维后的维数进行输入，两维或五维的输出形式进行识别。

4. 数据检测及分析

考虑到可比性及可操作性，本文选KDD99中的数据进行检测及分析。KDD99 数据集总共由500万条记录构成，它还提供一个10%的训练子集和测试子集，它的样本类别分布表如下：

标签类别

0 NORMAL: normal

1 PROBE: ipsweep, mscan, nmap, portsweep, saint, satan

2 DOS: apache2, back, land, mailbomb, Neptune, pod, processtable, murf ,teardrop, udpstorm

3 U2R: buffer_overflow, httptunnel, loadmodule, perl, ps, rootkit, sqlattack, xterm

4 R2L: ftp_write, guess_passwd, imap, multihop, named, phf, sendmail, snmpgetattack, snmpguess, spy, warezclient, warezmaster, worm, xlock, xsnoop

即此处将攻击类型分为 5 类分别用 0, 1, 2, 3, 4 表示

1) 数据预处理

①对protocol_type. 协议类型，离散类型，共有3 种：将TCP 替换为2, UDP替换为1，ICMP替换为0。

②对service. 目标主机的网络服务类型，离散类型，共有70 种：将ecr_i替换为3，将http替换为2，将private替换为1，其他67 种类型因为出现次数较少，均替换为0。

③对flag. 连接正常或错误的状态，离散类型，共11种：将SF 替换为1，其他10种均替换为0。

④对数据进行标准化。在 Matlab 中，标准化函数主要有两种 mapminmax(该函数是将数据的原始值除该数据中的最大值与最小值之差)和 zscore(该函数是将数据的原始值除该数据的标准差)。

2) 数据测试

KDD99 中的数据大约 500 万条连接记录，其中有大量的正常网络流量及几种具有代表性的攻击类型。攻击类型分别为：DOS 类攻击(拒绝服务攻击)、R2L 类攻击(远程权限获取)、U2 类攻击(各种权限提升)及 PROBE 类攻击(各种端口扫描和漏洞扫描)。由于原始数据数量过大，本文采用先对原始数据进行预处理，而后随机选取 10%的数据作为训练集(其中含攻击类型 22 种)，随机选取 32 万条数据作为测试集(其中含攻击类型 39 种)。利用 MATALAB7.0 进行计算测试，训练集取 10%，对数据进行标准化(标准化函数用 mapminmax)后，直接利用 SVM 模型，且模型中的参数 c 取 128，参数 g 取 0.5，分类只分两类，则对测试集的分类准确率为 92.717%，虚警率为 0.781%，误警率为 5.892%；训练集取 10%，对数据进行标准化(标准化函数用 zscore)后，SVM 模型中的参数 c 取 128，参数 g 取 0.5，则对测试集的分类准确率为 91.937%，虚警率为 0.792%，误警率为 5.906%；

对训练集先利用非线性投影方法分别将基本属性集的 9 种属性投影变为二维，内容属性集中的 13 种属性投影变为二维，流量属性集中的 9 种属性投影变为二维，主机流量属性集中的 10 种属性投影变为二维，而后利用带罚函数的 SVM 模型(核函数取径向基核函数)进行检测，其结果为：

随机的选取50,000条数据进行训练，分类为五类，则准确率为95.346%，虚警率为0.13%，误警率为2.73%：**Accuracy = 95.364% (47682/50000) (classification)**

xujing = 0.0013

wujing = 0.0273

通过主成分分析选取其中的10个属性来进行处理：

得到的结果如下：

Accuracy = 91.259% (283842/311029) (classification)

xujing = 0.0088

wujing = 0.0919

从以上计算来看，将各属性集利用投影寻踪法变为二维时，其入侵检测效果较好一些。

5. 结论

本文提出了利投影寻踪法对网络入侵数据进行降维，而后利用带罚函数的 SVM 模型对降维后的数据进行分类检测。从对 KDD99 中的数据的检验来看，效果较为理想。当然，由于对数据的降维还需进一步的考虑，如降多少维合适？如何降维？是线性降维还是非线性降维？等等，只有确定合适的降低维数，才能提高分类识别率。同时，分类识别方法也需进一步的研究，以提高入侵检测率。只有在这两方面都有较好的突破，入侵检测率才会有更大的提高。

参考文献 (References)

[1] 戴英侠等 (2002) 系统安全与入侵检测. 清华大学出版社, 北京, 3.

[2] 李阳等 (2005) 入侵检测系统在网络安全中面临的挑战及对策. 网络安全技术与应用, 北京.

[3] Yang, X.R., Shen, J.Y. and Wang, R. (2002) Artificial immune theory based network intrusion detection system and the algorithms design. *Proceedings of* 2002 *International Conference on Machine Learning and Cybernetics*, 73-77.

[4] Vapnik, V.N. (1995) The nature of statistical learning theory. Springer, New York.

[5] Spafford, E.H. and Zamboni, D. (2006) Intrusion detection using autonomous agents. *Computer Networks*, **34**.

[6] 吴庆涛, 路凯 (2009) 一种改进的基于因果关联的攻击场景重构方法. *微电子学与计算机*, **6**.

[7] 李健, 范万春, 何驰 (2005) 基于多分类向量机的网络入侵检测技术. *计算机应用*.

[8] Cai, T. and Shen, X.T. (2010) High-dimensional data analysis. 高等教育出版社, 10.