

基于独立成分分析和支持向量机的入侵检测方法

谷 雨¹, 郑锦辉², 孙 剑², 徐宗本²

(1. 西安交通大学电子与信息工程学院, 710049, 西安; 2. 西安交通大学理学院, 710049, 西安)

摘要: 提出了一种入侵检测方法, 该方法采用独立成分分析方法获取入侵行为模式的高阶统计信息, 并将输入模式空间映射到相应的独立成分空间, 然后利用支持向量机对小样本、高维数据泛化能力强的特点, 在独立成分空间中用支持向量机原理构造广义最优分类超平面. 数值实验表明, 所提方法可大大降低特征空间维数, 具有较好的分类正确性. 特别是当高斯核参数 σ 值在 1~3 之间时, 利用该方法的漏检数仅为标准支持向量机算法的 1/9, 这说明它能有效地获取入侵行为的本质特征, 对新的入侵行为有比较好的识别能力.

关键词: 入侵检测; 独立成分分析; 支持向量机

中图分类号: TP311 **文献标识码:** A **文章编号:** 0253-987X(2005)08-0876-04

Intrusion Detection Method Based on Independent Component Analysis and Support Vector Machine

Gu Yu¹, Zheng Jinhui², Sun Jian², Xu Zongben²

(1. School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;

2. School of Science, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: A novel intrusion detection method was presented, in which the independent component analysis approach was used to acquire the high order statistic information of intrusion action mode and mapped the input mode space into the corresponding independent component space. Then the generalized maximal margin hyperplane was constructed in the independent component space using the powerful feature of the support vector machine(SVM) for small samples and high dimension data generalization. Numerical simulation shows that the proposed method can reduce the dimension of the feature space, and has higher correct classification rate, especially, when the sigma of Gauss kernel is set to 1 to 3, the rate of false negative is just one ninth of the SVM's. It means that the intrusion detection method can effectively get the essential features of intrusion action and possess the higher ability to identify new intrusion activities.

Keywords: intrusion detection; independent component analysis; support vector machine

入侵检测(Intrusion Detection, ID)是对系统(网络)的运行状态进行监视,发现各种攻击企图、攻击行为或者攻击结果,以保证系统资源的可用性、完整性和机密性.从本质上讲,入侵检测是一种分类问题,它通过对训练集学习来构造分类器,将正常数据与异常数据分开.机器学习方法应用于入侵检测系统,能使系统具有更强的适应性、自学习性和鲁棒性,是目前入侵检测研究的一个重要方向^[1-3].但是,

这些方法常常强调入侵检测系统的分类正确率,而对漏检关注较少.对于一个安全系统而言,显然漏检数极为重要,它反映了系统的安全性受到威胁的可能性.

为了使入侵检测系统对新的入侵行为有更好的识别能力和识别效率,本文使用独立成分分析(ICA)先对入侵行为进行特征提取,然后对提取的特征数据应用支持向量机(SVM)原理构造入侵检

测分类器。

1 基于 ICA 特征提取和 SVM 的入侵检测方法

1.1 独立成分分析

独立成分分析是一种用于数据特征提取的线性变换技术,其方法描述如下。

设从 N 个通道获得的观测信号为 $\mathbf{X} = (x_1, x_2, \dots, x_N)^T$, 每个观测信号是 M 个独立源信号 $\mathbf{S} = (s_1, s_2, \dots, s_M)^T$ 的线性组合,即 $\mathbf{X} = \mathbf{AS}$, 其中 $\mathbf{A} = (a_{ij})_{N \times M}$ 为未知的混合矩阵。ICA 方法就是在混合矩阵 \mathbf{A} 和独立成分 \mathbf{S} 未知的情况下,根据观测数据 \mathbf{X} 确定分离矩阵 $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_M]^T$, 使得变换后的输出 $\mathbf{S}^* = \mathbf{A}^+ \mathbf{X} = \mathbf{WX}$ 是对 \mathbf{S} 的最优估计。根据信息论的知识,可采用负熵度量准则作为判断向量相互独立的标准^[4], 其表达式为

$$J_G(\mathbf{w}_i) = [E\{G(\mathbf{w}_i^T \mathbf{X})\} - E\{G(v)\}]^2 \quad (1)$$

其中 v 是标准高斯随机变量,函数 G 可以取

$$G_1(u) = \frac{1}{a_1} \lg(\cosh a_1 u), \quad 1 \leq a_1 \leq 2$$

$$G_2(u) = -\exp(-u^2/2)$$

采用牛顿法极大化式(1),可得到 ICA 的递推公式,即

$$\begin{aligned} \mathbf{w}_i^* &= E\{\mathbf{X}g(\mathbf{w}_i^T \mathbf{X})\} - E\{g'(\mathbf{w}_i^T \mathbf{X})\}\mathbf{w}_i \\ \mathbf{w}_i &= \mathbf{w}_i^* / \|\mathbf{w}_i^*\| \end{aligned} \quad (2)$$

其中 g 和 g' 分别是函数 G 的一阶、二阶导数。

1.2 SVM 原理

SVM 最早由 Vapnik^[5,6] 提出,是一种基于结构风险最小化原理的机器学习方法,主要思想是在保证经验风险 $R_{\text{emp}}(f)$ 尽可能小的前提下,极小化置信风险上界。它利用核函数将输入向量映射到一个高维特征空间,并在该空间内构造一个最优超平面来逼近分类函数。最优分类超平面的构造最终可以归结为二次规划问题,即

$$\left. \begin{aligned} \min_{\mathbf{w}, b, \xi} & \left(\frac{1}{2} \|\mathbf{w}\|^2 + C \sum_{i=1}^l \xi_i \right) \\ \text{约束: } & y_i (\langle \mathbf{w}, \Phi(\mathbf{x}_i) \rangle - b) \geq 1 - \xi_i \\ & \xi_i \geq 0, \quad i = 1, \dots, l \end{aligned} \right\} \quad (3)$$

该二次规划问题可以用对偶规划进行求解,即

$$\left. \begin{aligned} \max_{\alpha} & \mathbf{W}(\boldsymbol{\alpha}) = \sum_{i=1}^l \alpha_i - \frac{1}{2} \sum_{i=1}^l \sum_{j=1}^l \alpha_i \alpha_j y_i y_j K(\mathbf{x}_i, \mathbf{x}_j) \\ \text{约束: } & \mathbf{y}^T \boldsymbol{\alpha} = 0 \\ & 0 \leq \alpha_i \leq C, \quad i = 1, \dots, l \end{aligned} \right\} \quad (4)$$

式中: $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_l)^T$, α_i 为式(3)中不等式约束对应的 Lagrange 乘子; $K(\mathbf{x}_i, \mathbf{x}_j)$ 为核函数。

1.3 基于 ICA 和 SVM 的入侵检测方法

入侵检测问题本质上是希望确定一个判别函数 $f: R^n \rightarrow \{-1, +1\}$, 它能把输入数据集 $D = \{\mathbf{x}_i | i = 1, 2, \dots, l\} (\mathbf{x}_i \in R^n)$ 分为两类,即

$$f(\mathbf{x}_i) = \begin{cases} +1, & \mathbf{x}_i \text{ 为正常数据} \\ -1, & \mathbf{x}_i \text{ 为入侵数据} \end{cases}$$

因而是一个标准的分类问题。

在实际应用中,入侵数据包含大量属性项,然而入侵行为特征往往隐藏于少数几个属性中,冗余属性的存在反而会降低入侵检测的效果和效率,因此有必要对入侵数据进行特征提取。本文采用 ICA 方法消除输入数据的高阶相关性,将输入模式空间映射到相应的独立成分空间,从而有效地获得反映入侵行为特征的独立成分信息,然后用 SVM 的良好泛化性能在独立成分空间构造最优分类超平面,具体步骤如下。

步骤 1: 先对数据进行以下预处理。

(1) 中心化,即 $\mathbf{X} = \mathbf{X} - E\{\mathbf{X}\}$, 使得训练样本均值为 0。

(2) 白化,即 $\tilde{\mathbf{X}} = \mathbf{B}\mathbf{D}^{-1/2}\mathbf{B}^T\mathbf{X}$, 其中 \mathbf{B} 是 $E\{\mathbf{X} \cdot \mathbf{X}^T\}$ 的特征向量矩阵, \mathbf{D} 是特征值的对角矩阵(容易验证 $E\{\tilde{\mathbf{X}}\tilde{\mathbf{X}}^T\} = \mathbf{I}$)。

步骤 2: 根据式(2)迭代求出 ICA 变换的分离矩阵 \mathbf{W} , 并将训练数据映射到独立成分空间 \tilde{R}^m 中,即 $\mathbf{S} = \mathbf{WX}$, 其中 $s_i \in \tilde{R}^m, m \leq n$ 。

步骤 3: 在独立成分空间 \tilde{R}^m 中,应用 SVM 方法求出最优分类超平面。

步骤 4: 利用最优分类超平面分析入侵检测数据集。

2 实验分析

本文采用美国麻省理工大学林肯实验室提供的网络数据集 (http://kdd.ics.uci.edu/databases/kddcup99/kddcup.data_10_percent.gz), 通过随机无回放采样方法得到相互独立的训练数据集和测试数据集。训练数据集共有 1 000 条记录,包括正常数据和 13 种入侵类型数据,其中有 2 种入侵类型是该训练数据集独有的;测试数据集包含 9 000 条记录,分别属于正常数据和 17 种入侵类型数据,其中包含 6 种新的入侵行为。

实验采用漏检 N (未检测出的攻击次数)、分类正确率 η_1 (正确分类样本数与训练集样本总数之

比)和虚警率 η_2 (错分为异常的正常样本数与识别为异常的样本总数之比)对入侵检测分类器的效果进行评价。

在支持向量机的学习中,核函数的类型及其参数的选择对支持向量机的学习性能有重要影响,但如何选择合适的参数,目前还没有统一的标准.本文主要通过数值实验的方法进行模型选择,下面将通过2组数值实验来说明这一点。

仿真实验1 在不同特征维数下,基于ICA和SVM(ICA & SVM)的高斯核与多项式核的性能比较。

分别采用2种常用核函数——高斯核和多项式核,对标准SVM和不同特征维数下的ICA & SVM进行了性能比较,其中错分惩罚因子 $C=50$,实验结果如表1所示。

从实验中可以看出,当测试数据集中出现新的入侵行为时,标准SVM和ICA & SVM对新入侵行为的识别能力有很大差别,这主要体现在漏检数上.前者的漏检数比后者高得多,如在高斯核参数 $\sigma=3$ 时,采用标准SVM算法的入侵检测分类器有

208次入侵行为没有被检测出来,这在现实中是非常危险的,而采用9维独立成分的ICA & SVM算法仅有22次漏检.虽然较低的漏检数会使虚警率增高,但从网络安全角度考虑,这是值得的.采用9维独立成分,虚警率仅为6.7%,这也是可以接受的.同样,对于多项式核,ICA & SVM的漏检数也低于标准SVM.可见,所提新方法能有效地检测入侵行为,且在保持较低虚警率的情况下,对新的入侵行为有很好的识别能力。

从高斯核和多项式核的对比中还可以看到,在采用多项式核时,多项式的阶数 d 对入侵检测系统的性能影响非常大.当 $d=5$ 时,标准SVM方法和ICA & SVM方法的分类正确率骤降到50%以下,且ICA的特征维数与分类正确率不再相关,而当高斯核参数 σ 变化时,入侵检测系统的分类正确率稳定在一个可接受的范围内.从中可以看到,核参数的选择对分类器的性能有极大的影响。

仿真实验2 高斯核参数 σ 对入侵检测性能的影响。

表1 标准SVM与不同特征维数下的ICA & SVM 2种方法的性能比较

		标准 SVM	ICA & SVM			
			ICA 提取特 征维数为 3	ICA 提取特 征维数为 5	ICA 提取特 征维数为 7	ICA 提取特 征维数为 9
高 斯 核	N	189	11	25	27	28
	$\sigma=1$					
	$\eta_1/\%$	94.51	83.48	88.79	89.46	93.74
	$\eta_2/\%$	4.00	16.45	11.63	10.98	6.68
	N	203	12	19	17	21
	$\sigma=2$					
$\eta_1/\%$	94.41	83.49	89.16	89.92	93.44	
$\eta_2/\%$	3.95	16.44	11.33	10.62	7.07	
多 项 式 核	N	208	11	20	22	22
	$\sigma=3$					
	$\eta_1/\%$	94.36	83.51	89.43	90.70	93.79
	$\eta_2/\%$	3.95	16.43	11.06	9.82	6.70
	N	249	51	59	104	95
	$d=3$					
$\eta_1/\%$	95.96	82.91	87.39	88.39	93.97	
$\eta_2/\%$	1.44	16.63	12.63	11.28	5.70	
多 项 式 核	N	120	51	53	69	82
	$d=4$					
	$\eta_1/\%$	95.91	83.49	89.01	89.73	93.87
	$\eta_2/\%$	3.25	16.14	11.16	10.31	5.95
	N	4 534	64	6 750	7 377	7 336
	$d=5$					
$\eta_1/\%$	44.94	82.98	23.14	17.46	17.50	
$\eta_2/\%$	12.41	16.48	18.11	28.89	34.50	

从上面的对比实验中可看到,当支持向量机的核函数采用高斯核时,入侵检测的分类效果较好(采用漏检数与分类正确率作为综合评价指标),且具有较好的稳定性.下面通过实验对高斯核参数 σ 进行了研究,以考察不同的 σ 对入侵检测分类性能的影响.图 1~图 3 为漏检数、分类正确率和虚警率相对于高斯核参数 σ 的变化情况,其中 ICA & SVM 方法的独立成分特征维数是 9,错分惩罚因子 $C=50$.

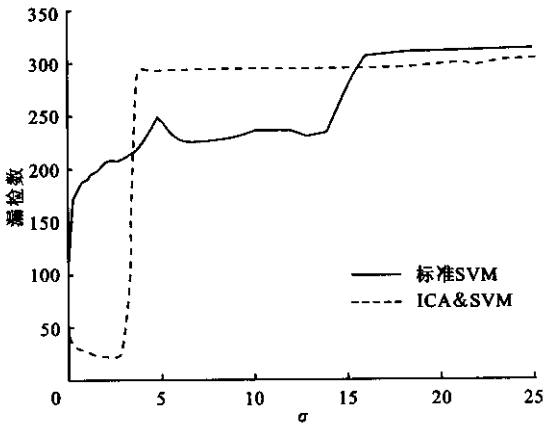


图 1 高斯核参数 σ 对漏检数的影响

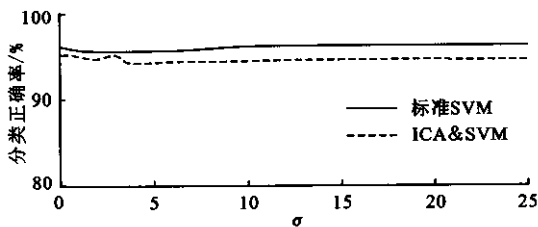


图 2 高斯核参数 σ 对分类正确率的影响

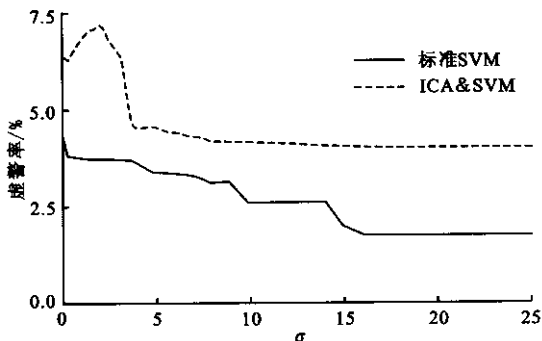


图 3 高斯核参数 σ 对虚警率的影响

从仿真实验 1 和实验 2 可以看出,高斯核参数 σ 在很大范围内变化时,入侵检测系统的分类正确率均在 93% 以上(见图 2),比多项式核具有更好的

稳定性.同时,采用标准 SVM 方法的分类器,其漏检数受高斯核参数 σ 的影响很大(见图 1),而采用 ICA & SVM 方法则变化比较平稳,相对而言,所提方法对核参数 σ 的选择不太敏感.

实验表明,在高斯核参数 $1 \leq \sigma \leq 3$ 时,采用 ICA & SVM 方法的入侵检测分类器的漏检数远远低于标准 SVM 方法,而且其虚警率约为 7%,是可以接受的.这说明,采用 ICA & SVM 方法的入侵检测分类器不仅能有效地获取入侵行为的本质特征,而且对新的入侵行为也有很好的识别能力.

3 结 论

通过采用独立成分分析方法来获取入侵行为特征之间的高阶统计信息,并将数据映射到相应的独立成分空间,然后通过支持向量机学习算法在独立成分特征空间中构造广义最优分类超平面.实验表明,这一方法大大降低了特征空间的维数,并有很好的分类正确率,而且漏检数比直接利用标准 SVM 方法低得多.这说明,在独立成分空间中可以用更少、更有效的特征来表示入侵行为数据.由于各独立成分之间具有高阶独立性,所以得到的分类器具有很强的泛化能力,对新入侵行为有良好的识别能力.

参考文献:

- [1] Liu Yanheng, Tian Daxin, Wang Aimin. ANNIDS: intrusion detection system based on artificial neural network [A]. 2003 International Conference on Machine Learning and Cybernetics, Xi'an, China, 2003.
- [2] Kumar S. Classification and detection of computer intrusions [D]. PhD Thesis. West Lafayette, USA: Department of Computer Science, Purdue University, 1995.
- [3] Zhao Junzhong, Huang Houkuan. An evolving intrusion detection system based on natural immune system [A]. 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering, Beijing, China, 2002.
- [4] Hyvärinen A, Oja E. Independent component analysis: algorithms and applications [J]. Neural Networks, 2000, 13(4-5): 411-430.
- [5] 瓦普尼克. 统计学习理论的本质 [M]. 张学工,译. 北京:清华大学出版社,2000.
- [6] 李 辉,管晓宏,咎 鑫,等. 基于支持向量机的网络入侵检测[J]. 计算机研究与发展,2003, 40(6): 799-807.