

融合 PCA 和 LDA 的入侵检测算法

张瑞霞,王 勇

(桂林电子科技大学 计算机与控制学院,广西 桂林 541004)

摘 要:针对目前单个 IDS 在入侵特征提取和检测效率上存在的问题,提出了一种融合主成分分析(PCA)和线性判别分析(LDA)的入侵检测算法。利用 PCA 和 LDA 提取入侵特征,通过 KNN 分类器给出初步的识别结果,接着采用 D-S 证据理论对识别结果进行融合,得出最终识别结果。通过在 KDD CUP'99 的标准入侵检测数据集上的实验表明,该方法提高了入侵检测率,同时降低了误报率,性能优于单一的分类器。

关键词:入侵检测;主成分分析;线性判别分析;D-S 证据理论;分类器融合

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2009)11-0132-03

Fusion of PCA and LDA for Intrusion Detection

ZHANG Rui-xia, WANG Yong

(Dept. of Computer and Control, Guilin University of Electronic Techn., Guilin 541004, China)

Abstract: To solve the difficulty of feature extraction and the low performance in single IDS, an intrusion detection method based on the fusion of principal component analysis(PCA) and liner discriminate analysis(LDA) is presented. Firstly, PCA and LDA is applied to network intrusion feature extraction. Then, initial intrusion detection result is done by two KNN classifiers. Next, the D-S evidence theory is adopted to fuse these results for two classifiers can overcome the shortcomings of each other. Experiment has been done on dataset in KDD-99 and the results show that the performance of the proposed method is superior to that of the single classifier.

Key words: intrusion detection; PCA; LDA; D-S evidence theory; classifiers fusion

0 引 言

入侵检测技术作为信息安全技术的一个重要方面得到迅速的发展。入侵检测问题实质上就是一个分类问题,它通过对训练集学习来构造分类器,将正常数据和异常数据区分开来。目前将模式识别技术应用到入侵检测中成为入侵检测领域研究的一个热点^[1,2]。国内看到的研究有文献[3,4]。特征选择和分类器的设计是入侵检测涉及的两个重要方面。

从模式识别的整个结构流程来看,特征选择的目就是尽可能保留分类信息的前提下,得到信息最大的特征,删除那些不利于分类或用途不大的信息或特征,特征选择的另一个目的是为了加快处理速度。在特征方面,入侵检测数据具有多维性的特点,但入侵行为往往只集中在少数几个属性项当中,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。主成分分析和线性判别分析能够对样本空间进行降维,从而使得匹配和识别在低维子空间进行^[5]。

分类器的设计与融合:虽然模式识别和入侵检测主要任务是设计一个高性能的 0-1 分类器,如果单个分类器提取的特征具有独立性和互补性,通过对现有的分类器融合获得比单个分类器更高的分类精度。正是由于这个原因,近年来,数据融合、分类器融合的方法越来越受到人们的重视,它的应用已经从军事领域越来越广泛地应用到民用领域,如机器人、人脸识别等。分类器融合的成功应用,使得研究人员从理论上分析了分类器融合的条件、提高识别率的原因以及融合的策略,从而给分类器融合提供了坚实的理论基础^[6-8]。另外根据笔者前期的研究^[9],应用 D-S 证据理论融合 HIDS 和 NIDS 达到了比较满意的性能。

基于这两方面的原因,提出了融合主成分分析和线性判别分析的入侵检测算法,首先通过 PCA 和 LDA 方法对数据获得分类结果,然后通过 D-S 证据理论将二者检测的结果融合处理,得到最终识别结果。仿真实验表明,该算法具有理想的检测率,漏检率低。

收稿日期:2009-03-11;修回日期:2009-06-17

基金项目:广西自然科学基金资助项目(桂科基 0575094)

作者简介:张瑞霞(1973-),女,河北石家庄人,讲师,硕士,研究方向为计算机信息与网络安全、入侵检测等;王 勇,教授,研究方向为信息与网络安全、分布式入侵检测系统等。

1 PCA 方法、LDA 方法和 D-S 证据理论

1.1 主成分分析和线性判别分析

主成分分析是通过 K-L 变换将训练样本集中的数据得到彼此正交互不相关特征。它使用了最大的几个特征值对应的特征向量组成变换矩阵,这些特征向量(基向量)构成一个子空间,基向量对应着原始空间变化最大的方向。

主成分分析按照公式(1)中的线性变换把图像 X 投影到低维空间中的向量 Y :

$$Y = W^T X \quad (1)$$

式中, $X \in R^N$, $Y \in R^M$ ($N \gg M$), W 代表投影矩阵。令 N 维向量 X_i ($i = 1, 2, 3, \dots, L$) 代表样本数据的 L 个属性特征,代表它们的平均。则样本的协方差矩阵定义为:

$$W_{PCA} = \frac{1}{L} \sum_{i=1}^L [(X_i - \mu)(X_i - \mu)^T] \quad (2)$$

主成分分析投影矩阵的列向量则是由 W_{PCA} 的对应前 M 个最大特征值的特征向量组成。

该方法的最优性是从 N 个训练样本中提取 m 个主要特征,来达到降维的目的。但是从表示的角度创建子空间,没有考虑到类内、类间的差异。线性判别分析方法正好弥补了这个缺点。线性判别分析的投影矩阵通过最大化类间分布,同时最小化类内散布获得,包含了类可分性信息,因此它所形成的特征能最大限度地不同的类别区分开来。

令 $X_k^{(i)}$ 为第 k ($k = 1, 2, \dots, C$) 类的第 i 个测试样本, μ_k 为第 k 类的样本平均,则类间散布矩阵可表示为:

$$S_B = \frac{1}{L} \sum_{k=1}^q [N_k(\mu_k - \mu)(\mu_k - \mu)^T] \quad (3)$$

类内散布矩阵可以表示为:

$$S_W = \frac{1}{L} \sum_{k=1}^c \sum_{i=1}^{N_k} [X_k^{(i)} - \mu_k)(X_k^{(i)} - \mu_k)^T] \quad (4)$$

其中, N_k 是第 k 类的样本数。

1.2 D-S 证据理论

证据理论^[10]又称为 Dempster-Shafer 理论,是一种不确定性推理方法。与传统的概率论相比,D-S 理论能更好地把握问题的未知性与不确定性,常用于信息融合^[11]。D-S 证据理论用识别框架 Θ 表示感兴趣的命题集,其上的布尔代数是分割组成的集类 R ,在其上定义基本概率赋值(BPAF - basic probability assignment):满足:

$$\sum |m(A), A \subseteq \Theta| = 1, m(\emptyset) = 0$$

其中, $m(A)$ 表示证据支持命题 A 发生的程度,而不支持任何 A 的真子集。 \emptyset 代表空集。

证据理论通过合成公式来合成多个证据源提供的证据。设有 n 个分类器,各分类器相应的基本概率赋值函数为 $m_i(A_j)$,表示第 i 个分类器对第 j 命题的后验可信度分配,则证据理论基本合成公式为:

$$\begin{aligned} m(\emptyset) &= 0 \\ m(P) &= c^{-1} \sum_{\substack{A_j \neq \emptyset \\ \cap A_j \neq \emptyset}} \prod_{i=1}^n m_i(A_j) \end{aligned} \quad (5)$$

$$\text{其中, } c = \sum_{\substack{A_j \neq \emptyset \\ \cap A_j \neq \emptyset}} \prod_{i=1}^n m_i(A_j)$$

决策规则定义:具有最大可信度的目标类别;目标类别的可信度值与其它类别的目标可信度值相差超过某一阈值(具体见算法定义);目标类别的可信度值必须大于不确定区间的可信度。

2 融合 PCA 和 LDA 的入侵检测

2.1 应用 D-S 证据理论融合分类器

对测试数据,从中分别提取出 PCA 和 ICA 两种特征,经过一个距离权重 K-NN 分类器后得到一个识别结果,将这两个分类器的输出作为两条证据,利用证据理论合成规则对它们进行融合,根据决策规则得到一个最终的识别结果。如图 1 所示。

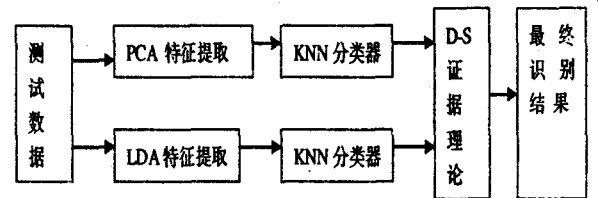


图 1 融合 PCA 和 LDA 的入侵检测

2.2 基本概率赋值的构造

基本概率赋值的构造是应用 D-S 证据理论融合涉及的一个重要问题。下面论述如何将 K-NN 分类器的输出转化为证据理论中的基本概率赋值。

考虑到一个 K-NN 分类器在做出最后决策之前对最多 K 个类别都有一定的支持度,该支持度与前面得到的距离权重相对应。为了提供更多的分类信息,将归一化的距离权重作为 K-NN 分类器的输出。同时由于分类器的输出不是完全可信的,将不可信的部分赋值给整个的框架。假设在一个测试集上得到的两个距离权重 K-NN 分类器的正确分类率分别为 ϵ_r^{PCA} 和 ϵ_r^{LDA} ,它们对整个识别框架的支持度分别为 $1 - \epsilon_r^{PCA}$ 和 $1 - \epsilon_r^{LDA}$ 。

设入侵类别总数为 M 类,令识别框架 $\Theta = \{T_1, T_2, \dots, T_M\}$ 。给定一个测试数据,设对应于 PCA 特征的与其最近邻的 K 个入侵样本对应的类别数为 K'_1 ($K'_1 < K$),对应的权重分别为 $d_1^{PCA}, d_2^{PCA}, \dots, d_{K'_1}^{PCA}$,将这 K'_1 个距离权重归一化,并转化到 M 个类别变成

$w_1^{pca}, w_2^{pca}, \dots, w_M^{pca}$, 其中只有 K'_1 个不为零。同理, 对应 LDA 特征的与其最近邻的 K 个入侵样本对应的类别数为 $K'_2 (K'_2 < K)$, 对应的权重分别为 $d_1^{lda}, d_2^{lda}, \dots, d_{k'_2}^{lda}$, 将这 K'_2 个距离权重归一化, 并转化到 M 个类别变成 $w_1^{lda}, w_2^{lda}, \dots, w_M^{lda}$ 。

对应该测试数据, 两个分类器给出的两条证据的基本概率分配如下:

$$m_{pca}: m_{pca}(T_1) = \epsilon_r^{pca} w_1^{pca}, m_{pca}(T_2) = \epsilon_r^{pca} w_2^{pca}, \dots, m_{pca}(T_M) = \epsilon_r^{pca} w_M^{pca}, m_{pca}(\Phi) = 0, m_{pca}(\Theta) = 1 - \epsilon_r^{pca}$$

$$m_{lda}: m_{lda}(T_1) = \epsilon_r^{lda} w_1^{lda}, m_{lda}(T_2) = \epsilon_r^{lda} w_2^{lda}, \dots, m_{lda}(T_M) = \epsilon_r^{lda} w_M^{lda}, m_{lda}(\Phi) = 0, m_{lda}(\Theta) = 1 - \epsilon_r^{lda}$$

2.3 入侵检测算法

2.3.1 训练过程

(1) 给定一类入侵的训练集 $X_i, i = 1, 2, \dots, N$, 根据公式(2) 计算协方差矩阵, 然后求其 m 个最大特征值对应的特征向量构成 PCA 特征投影矩阵 W_{pca} , 即 PCA 特征数据库。

(2) 直接运用 LDA 算法无法直接求出 $S_W^{-1} S_B$ 的特征向量。本算法利用 PCA 投影矩阵 W_{pca} 获得 m 维 MEF 最佳特征描述, 即 $(y_1^i, y_2^i, \dots, y_m^i)^T = W_{pca}^T (x_i - \bar{m}_i - m_0)$, 其中, $i = 1, 2, \dots, N$ 。

(3) 利用 $(y_1^i, y_2^i, \dots, y_m^i)^T$ 计算 S_W, S_B 和对应矩阵 $S_W^{-1} S_B$ 的 k 个最大特征值对应的特征向量构成的 FLD 投影矩阵 W_{fld} , 然后将其转换为 k 维 MDF 空间, 得到 LDA 的分类特征 $W_{lda} = W_{fld}^T y_i$, 即 LDA 特征数据库。

(4) 计算每两类之间的距离并取其最大值的一半作为距离阈值, 分别为 T_{pca} 和 T_{lda} 。

(5) 归一化处理 T_{pca} 和 T_{lda} :

$$TF_{pca} = \frac{T_{pca}}{T_{pca} + T_{lda}}, TF_{lda} = \frac{T_{lda}}{T_{pca} + T_{lda}}$$

2.3.2 单个分类器的正确分类率

(1) 通过训练过程的方法求出测试样本集 1 的 PCA 特征和 LDA 特征。

(2) 计算测试样本集 1 到各类训练样本投影特征的 KNN 距离, 分别是 $d_1^{pca}, d_2^{pca}, \dots, d_{k'_1}^{pca}$ 和 $d_1^{lda}, d_2^{lda}, \dots, d_{k'_2}^{lda}$ 。

(3) 分类依据:

$$h = \arg \min(d_i^{pca}) \text{ and } (d_i^{pca} < T_{pca})$$

$$h = \arg \min(d_i^{lda}) \text{ and } (d_i^{lda} < T_{lda})$$

表示最终把测试样本判为 h 类。

(4) 得到在测试集 1 上正确分类率为 ϵ_r^{pca} 和 ϵ_r^{lda} 。

2.3.3 证据理论融合过程

(1) 在测试集 2 上重复 2.3.2 的(1)和(2)步。

(2) 将距离权重归一化处理, 并转化到 M 个类别, 得到两个分类器给出的两条证据的基本概率分配。

(3) 利用证据合成公式(5) 融合两条证据得到 $m(P_i) i = 1, 2, \dots, M$ 。

(4) 融合后的分类依据:

$$g = \arg \max(m(P_i)) \text{ and } (m(P_i) > TF_{pca}) \text{ and } (m(P_i) > TF_{lda})$$

g 表示最终把测试样本判为 g 类。

3 仿真实验

采用 MIT 林肯实验室公开提供的 DARPA 入侵检测评价计划中的网络通信数据集, 经过处理后形成的 KDD Cup'99 Data 训练数据集进行仿真。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。数据集中每条数据有 42 个特征, 其中最后一条为攻击的类型特征, 该特征分为 5 类, 分别用 0 表示正常, 1 表示 DOS 攻击, 2 表示 PRB 攻击, 3 表示 U2R 攻击, 4 表示 U2L 攻击。

定义证据理论中的识别框架 $\Theta = \{\text{DOS}, \text{PRB}, \text{U2R}, \text{U2L}, \text{UNKNOWN}\}$

在 41 个特征属性中, 其中 7 个为符号变量, 34 个为数值变量。以 34 个数值变量为分析对象, 进行主成分分析和线性鉴别分析。在仿真实验中, 把测试数据集分类训练, 测试数据集有 2 个, 一个用于获得单个分类器的初始识别率, 一个用于融合方法的测试。

表 1 给出了 D-S 证据理论融合的可信度对比。表 1 表明融合单个分类器后, 提高了攻击类型的分类可信度, 降低了不确定性的可信度。表 2 和表 3 分别给出了应用证据理论的识别率和误报率。为了方便比较, 同时给出了 PCA 和 LDA 方法的 KNN 分类器结果以及融合后情况。表 2 和表 3 的实验结果表明, 采用融合的方法比使用单个特征分类器的检测率的最好情况提高了 2 个百分点, 同时比使用单个特征分类器的误报率的最好情况降低了 2 个百分点。

表 1 应用证据理论融合单个分类器

实际攻击	Classifier	DOS	PRB	U2R	U2L	UNKNOWN
DOS	PCA	0.56	0.23	0.08	0.06	0.07
DOS	LDA	0.35	0.35	0.10	0.07	0.13
DOS	FUSION	0.61	0.28	0.05	0.05	0.01

表 2 检测率比较

Classifier	DOS	PRB	U2R	U2L	Average
PCA	0.912	0.944	0.939	0.942	0.934
LDA	0.905	0.953	0.961	0.966	0.945
FUSION	0.955	0.964	0.972	0.971	0.965

(下转第 138 页)

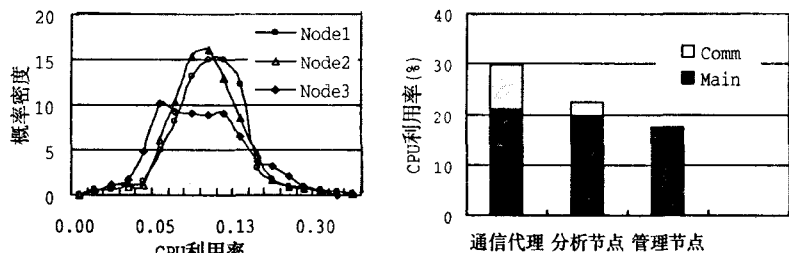


图 3 实验结果

5 结束语

给出了一个在普通硬件条件下建立的可扩展、高性能的网络入侵检测系统,该入侵检测系统由一个分发网络流量的前端分发节点及一个可扩展的分析节点群组成。每一个分析节点对其接收到的数据进行入侵检测,并在需要时和集群系统同步状态和检测信息。该集群系统对于使用者是透明的,感受如同使用单一入侵检测系统。

在集群系统的建立过程中,着重讨论了前端分发节点的多种流量分发策略,最后对该集群系统进行的测试说明其达到了透明、可扩展、易于维护、经济的目标。

对入侵检测系统分析算法的改进使其更加适合分布式的集群系统,减少分析节点间内部数据的交换,有待进一步地研究。

参考文献:

- [1] 甘学士,孙力娟.改进的模式匹配算法及在入侵检测中的应用[J].计算机技术与发展,2006,16(7):150-152.
- [2] 高志森,张铮,李俊.入侵检测中贝叶斯分类器改进的研究[J].计算机技术与发展,2006,16(11):154-155.
- [3] 杨武,方滨兴,云晓春,等.基于骨干网的并行集群入侵检测系统[J].哈尔滨工业大学学报,2004,36(3):273-276.
- [4] 张丹慧,佟振声.基于Agent与数据挖掘的分布式入侵检测系统[J].微机发展(现更名:计算机技术与发展),2004,14(3):125-126.
- [5] 徐长棣,刘方爱.基于P2P和移动代理的入侵检测系统研究[J].计算机技术与发展,2007,17(1):164-166.
- [6] Vigna G, Eckmann S T, Kemmerer R A. The STAT Tool Suite[C]//In:Proc. DARPA Information Survivability Conference and Exposition. [s.l.]:[s.n.],2000.
- [7] Blanc M, Oudot L, Glaume V. Global Intrusion Detection: Prelude Hybrid IDS[R]. [s.l.]:[s.n.],2003.
- [8] Zhiruo C, Zheng W, Zegura E. Performance of Hashing-Based Schemes for Internet Load Balancing[M]. Piscataway: [s.n.],2000:332-341.
- [9] Kohler E, Morris R, Chen B, et al. The Click modular router [J]. ACM Transactions on Computer Systems,2000,18(3):263-297.

(上接第 134 页)

表 3 误报率比较

Classifier	DOS	PRB	U2R	U2L	Average
PCA	0.033	0.028	0.032	0.032	0.031
LDA	0.039	0.038	0.035	0.032	0.036
FUSION	0.017	0.028	0.025	0.018	0.011

4 结束语

通过在决策级融合单分类器的检测结果,提高了检测率,同时降低了误报率。进行特征级融合是今后的研究方向。

参考文献:

- [1] Labid K, Venuri V R. Application of Principal Component Analysis to the Detection and Visualization of Computer Network Attacks[M]//Annals of Telecommunications. France: [s.n.],2005.
- [2] Shyu M L, Chen S C, Sarinapakorn K, et al. A Novel Anomaly Detection Scheme Based on Principal Component Classifier[C]//Proceedings of ICDM Foundation and New Direction of Data Mining workshop. [s.l.]:[s.n.],2003:172-179.

- [3] 王坤,潘继农,张鹏,等.基于主成分分析的异常检测方法研究[J].信息工程大学学报,2004,5(3):56-59.
- [4] 谷雨,邓锦辉,孙剑,等.基于独立成分分析和支持向量机的入侵检测方法[J].西安交通大学学报,2005,39(8):876-879.
- [5] 田捷,杨鑫.生物特征识别技术理论与应用[M].北京:电子工业出版社,2004.
- [6] Kuncheva L. A theoretical study on six classifier fusion strategies[J]. IEEE Trans on PAMI,2002,24(2):281-286.
- [7] Kitter J, Hatef M, Duin R, et al. On combining classifiers[J]. IEEE Trans on PAMI,1998,20(3):226-239.
- [8] David M J. Combining multiple classifiers by averaging or by multiplying[J]. Pattern Recognition,2000,33:1475-1485.
- [9] 王勇,王行愚,张瑞霞.基于D-S证据理论的分布式入侵检测方法研究[J].计算机工程与应用,2004(13):167-169.
- [10] 徐耀红.数据融合理论与应用[M].西安:西安电子科技大学出版社,1998.
- [11] 孙即祥.现代模式识别[M].长沙:国防科技大学出版社,2003.