

## 基于贝叶斯的入侵检测模型与仿真研究

章 倩<sup>1</sup>, 周 健<sup>2</sup>

(1 合肥工业大学 计算机与信息学院, 安徽 合肥 230009; 2 合肥工业大学 信息与网络中心, 安徽 合肥 230009)

**摘 要:** 本文提出了一种基于贝叶斯的网络入侵检测模型. 首先, 使用主成分分析法提取网络数据包关键属性、消除冗余属性、降低维数, 再用贝叶斯分类器进行分类. 结果表明, 该模型不但提高了入侵检测的效率, 而且也加快了检测速度, 更适合当前的复杂网络检测.

**关键词:** 网络安全; 网络入侵; 主成分分析; 贝叶斯分类器

**中图分类号:** TP393

**文献标识码:** A

**文章编号:** 1000-7180(2013)11-0119-04

## The Intrusion Detection Model and Simulation Study Based on the Bayesian

ZHANG Qian<sup>1</sup>, ZHOU Jian<sup>2</sup>

(1 School of Computer and Information, Hefei University of Technology, Hefei 230009, China;

2 Information and Network Center, Hefei University of Technology, Hefei 230009, China)

**Abstract:** This paper proposes a network intrusion detection model based on Bayesian. First, the principal component analysis (PCA) was used to extract the key ability, eliminate the redundant attributes, reduce the data dimension, then use the Bayesian classifier to classify. The simulation results show that the model improves the efficiency of the intrusion detection and speed up the detection speed, and is suitable for the current complex network intrusion detection.

**Key words:** network security; network intrusion; PCA; Bayesian classifier

### 1 引言

网络已经成为人们生活不可或缺的一部分, 由此所引起的网络安全问题也已成为人们研究的重要课题. 入侵检测系统, 作为继防火墙后的网络第二道防线, 也越加受到人们的重视<sup>[1]</sup>.

入侵检测技术主要对通过的数据包加以检测, 目前主要研究是异常入侵检测, 它是在用户或者系统与外部建立一种模型, 然后通过模型对要求经过的数据包加以分析, 判断是否有异常行为, 通常能够检测出已有的或者未知的入侵行为. 网络数据包中携带着极其丰富的各类信息, 这些不相关的冗余特征使得网络监测变得越来越复杂, 并且入侵手段日趋高维性、多样性、复杂性. 传统的入侵检测技术<sup>[2]</sup>

在处理高维数据时, 效率低下, 用于当前的大规模的入侵检测显然是不适合的. 近年来, 将数据挖掘技术引入到入侵检测中, 已成为入侵检测的主要方向, 也已得到很多的研究成果, 文献[3]中, 由于对数据没有进行处理, 从而导致训练时间过长; 文献[4]提出的方法, 对特征进行选择, 却无法去除冗余特征. 本文将主成分分析法与贝叶斯分类器相结合, 得到一种更为高效的入侵检测方法, 不论是效率还是速度都有一定程度的突破.

### 2 主成分分析—贝叶斯的入侵检测方法

#### 2.1 算法分析

入侵检测作为网络安全体系结构中的一个重要组成部分, 旨在对那些未授权的试图破坏网络资源

收稿日期: 2013-01-26; 修回日期: 2013-03-06

基金项目: 国家自然科学基金项目(60873194)

机密性、完整性和可用性的入侵行为进行检测,进而采取相应的应对措施.而当前的入侵检测算法存在以下不足:检测效率低,误报率高,漏报率高,检测速度慢等<sup>[5]</sup>.因此,提高效率和准确率显得尤为重要.本文主要采用了以下两种手段弥补以上的不足,第一:进行特征选择;第二:分类模型的选择以及参数优化<sup>[6]</sup>,所使用的方法为主成分分析和贝叶斯网络.

主成分分析的目的就是通过实验,在训练集中选取较少量的关键因子,去除那些无关的或者影响很小的因子,剩余的关键因子能够反映和解释观测事实.贝叶斯网络建立在贝叶斯理论的基础上,有着稳固的数学理论支持,它以计算得到的概率权重来描述数据间的关系.针对高维、多样、复杂的入侵行为,过多的属性反而使得分类效率低下,导致较高的误报率和漏报率.因此,降低属性维数显得至关重要.对降低维数所得到的属性,利用贝叶斯网络进行分类,进而判断是否有人入侵行为,由于贝叶斯网络有着较好的分类功能,选择贝叶斯网络进行分类显然是合适的.其模型流程如图 1 所示.

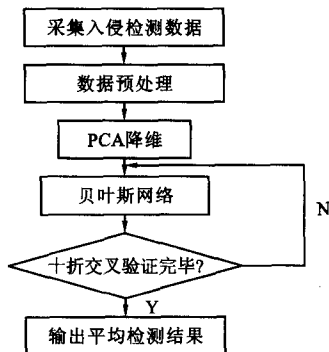


图 1 网络入侵检测工作流程图

## 2.2 主成分分析

主成分分析是一种把原来多个因子转换为少数几个相互独立的关键因子的统计方法.从概率的角度来剔除那些冗余属性和携带信息少的属性,然后用获得的关键因子描述原数据集,以达到降维的目的.设  $X_1, X_2, \dots, X_n$  为原本属性集,需求属性为  $Y_1, Y_2, \dots, Y_m$ ,则要求  $m < n$  且  $Y_1, Y_2, \dots, Y_m$  相互独立,即要求  $\text{COV}(Y_i, Y_j) = 0$ ;  $D(Y_i)$  较大.那么,这  $m$  个新的变量能够代表原来的  $n$  个变量描述原本数据集的大部分信息.算法具体步骤如下:

(1) 记  $X = (X_1, X_2, \dots, X_n)$ ,  $X_i = (X_{1i}, X_{2i}, \dots, X_{pi})^T$ ,  $p$  为观察的次数,将原始数据矩阵  $X$  标准化,仍记为  $X$ .

(2) 根据  $X$ , 计算相关矩阵

$$R = (r_{ij})_{n \times n} = X^T X.$$

(3) 根据相关矩阵  $R$ , 计算  $R$  的特征方程  $\Delta(R - \lambda E) = 0$  求出特征根  $\lambda_1, \lambda_2, \dots, \lambda_n$  不妨设  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n > 0$ .

(4) 根据实际要求  $|R|$  取值来确定所需关键因子  $m$  的值:

$$\frac{\sum_{i=1}^m \lambda_i}{\sum_{i=1}^n \lambda_i} \geq |R|.$$

(5) 根据所需的  $m$  个关键因子,计算选入的  $\lambda_i$  所对应的特征向量  $e_i$ .

(6) 计算  $Y_1, Y_2, \dots, Y_m$ , 其中有  $Y_i = e_{1i}X_1 + e_{2i}X_2 + \dots + e_{mi}X_m, i = 1, 2, \dots, m$ .

根据以上步骤,则可以根据实际要求找出能够描述原数据集的最大关键因子数  $m$  的值,然后用这  $m$  个关键因子重新描述原本数据集,从而达到降维的目的.

## 2.3 贝叶斯网络

利用贝叶斯网络进行分类,主要是依据贝叶斯定理,贝叶斯网络是当前解决不确定性知识推理的主要方法.贝叶斯网络在进行分类时,利用概率的权重来描述样本中数据之间的相关性,最终以最大的概率权重来判别一组数据的类别,具有高的分类效率.贝叶斯网络由于其不确定知识表达形式、概率的计算,结合先验知识学习特征来进行判别,基于这一点,可以很好的引入到网络入侵检测当中.为了便于本文的理解,给出以下定义:

**定义 1** (贝叶斯定理) 设实验  $E$  的样本空间为  $S$ ,  $A$  为  $E$  的事件,  $B_1, B_2, \dots, B_n$  为  $S$  的一个划分,且  $P(A) > 0, P(B_i) > 0 (i = 1, 2, \dots, n)$ , 则

$$P(B_i | A) = \frac{P(A | B_i)P(B_i)}{\sum_{j=1}^n P(A | B_j)P(B_j)}$$

**定义 2** (贝叶斯网络) 设  $B = \langle G, \Theta \rangle$  为一个贝叶斯网络,其中  $G$  为有向无环图,  $G$  中结点为随机变量  $X_1, X_2, \dots, X_n$  的集合,这里将  $X_1, X_2, \dots, X_n$  定义为待检测数据集的属性集,  $G$  中的弧表示结点间的依赖关系.若存在弧  $X_i$  到弧  $X_j$ , 则  $X_i$  为  $X_j$  的双亲结点,  $X_j$  为  $X_i$  的孩子结点,并用  $Pa(X_k)$  表示所有的双亲结点,  $pa(x_k)$  为  $Pa(X_k)$  的一个取值.  $\Theta$  量化网络中的参数,  $\forall X_i, Pa(X_i)$  的取值,则存在一个参数  $x_i, pa(x_i) \theta_{x_i | pa(X_i)} = P(x_i | pa(X_i))$ , 图 2 所示为一个贝叶斯网络.

在前面进行主成分分析时,提取是几乎能完全描述原本数据集的关键因子,此外,这些关键因子是相互独立的.针对因子的这种特征,采用贝叶斯网络

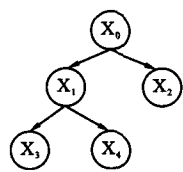


图2 一个贝叶斯网络

进行分类时,选择的是朴素贝叶斯网络.朴素贝叶斯网络是有约束的贝叶斯网络,它所要求的就是结点是相互独立的,而且在网络的建立过程以及学习过程中计算量比较少,所用时间比较短.

在主成分分析中,得到提取后的关键因子  $Y_1, Y_2, \dots, Y_m$ , 记  $Y = \{y_1, y_2, \dots, y_m\}$ , 其中  $y_1, y_2, \dots, y_m$  对应属性  $Y_1, Y_2, \dots, Y_m$  所取的值. 利用朴素贝叶斯分类步骤如下:

(1) 将入侵检测分类结果为  $C_1, C_2$ ,  $C_1$  表示安全,  $C_2$  表示入侵行为. 对于待检测的未分类数据样本  $Y$ , 计算  $Y$  属于具有最高后验概率(条件  $Y$  下)的类. 即当样本数据  $Y$  属于  $C_i$  时, 当且仅当

$$P(C_i | Y) > P(C_j | Y)$$
$$i \in \{1, 2\}, j \in \{1, 2\}, i \neq j$$

(2) 根据定义 1, 有

$$P(C_i | Y) = \frac{P(Y | C_i)P(C_i)}{P(Y)}$$

对于  $C_1, C_2, P(Y)$  值相同, 只需计算  $P(Y | C_i)P(C_i)$ , 由于  $Y_1, Y_2, \dots, Y_m$  相互条件独立,  $P(Y | C_i) = \prod_{k=1}^m P(y_k | C_i)$ , 而  $P(y_1 | C_i), P(y_2 | C_i), \dots, P(y_m | C_i)$  为训练样本估值.

(3) 为未知样本  $Y$  分类, 对于每个类  $C_i$ , 计算  $P(Y | C_i)P(C_i)$ . 样本  $Y$  为类  $C_i$ , 当且仅当

$$P(Y | C_i) > P(Y | C_j)$$
$$i \in \{1, 2\}, j \in \{1, 2\}, i \neq j$$

3 实验仿真与结果

本文采用 MIT 林肯实验室提供的经典入侵检测数据集 KDD CUP 99<sup>[7]</sup> 来进行实验. 该数据集含有 500 万条数据, 由于过于庞大, 按照一般的实验数据选取方法, 本文选取其中的 10% 的数据进行仿真实验. 数据集中的每条数据共有 42 条属性, 最后一个属性为分类标志. 统计所有的分类标志, 该数据集共有 5 种类型, 分别为正常、DOS 攻击、Probe 攻击、R2L 攻击和 R2R 攻击.

3.1 主成分分析

CUP 99 中的每条数据含有 41 条属性, 是典型的高维属性, 其中包含了一些无关属性, 为了去除这

些无关属性, 以及一些携带很少的信息的属性, 采用主成分分析进行降维. 实验中根据  $|R|$  的取值, 多次进行实验, 最终选择能够最大量描述原本数据集的 23 条属性作为最终的属性约简结果, 这 23 条属性能够描述原本数据集的 98.7%, 因此, 约简后的数据集基本等同于原本数据集, 从而提高了入侵检测的效率, 加快了检测速度.

3.2 贝叶斯网络分类

为了便于分类, 需要对数据集进行预处理, 首先将所有数据进行离散化, 其次, 将所有数据分为正常、DOS 攻击、Probe 攻击、R2L 攻击和 R2R 攻击、以及原本的所有数据依次进行实验. 本文采取的是十折交叉验证算法, 该算法共进行十次实验, 每次将数据集分成十份, 轮流将其中九份作为训练集, 一份作为测试集, 最终取十次结果的平均值作为最后的结果.

首先, 对未进行降为的数据以及降维后的数据各自进行实验比较. 实验结果如表 1 所示. 可以明显看出, 未降维的数据集分类效果低下, 说明原本的无关属性、冗余属性在进行类别判断时反而影响了判断结果; 降维后的数据选取的都是关键因子, 没有无关属性的影响, 判断结果大大提高.

其次, 依次将数据集进行其他算法的实验分类, 这里选取的主要是神经网络方面的相关算法, 采用相同的数据集, 经过多次试验比较, 得到如表 2 所示的结果. 经比较可以发现, 本文算法相对于其他算法, 在判别效率上有了很大的提高.

表 1 降维前后的比较

| 数据类别   | 未处理/% | 处理后/% |
|--------|-------|-------|
| NORMAL | 85.8  | 99.9  |
| U2R    | 23.7  | 82.7  |
| DOS    | 97.3  | 99.9  |
| R2L    | 93.4  | 99.7  |
| PROBE  | 87.3  | 95.3  |
| TOTAL  | 96.1  | 99.7  |

表 2 不同模型的比较

| 试验方法         | 正确率/% | 错误率/% |
|--------------|-------|-------|
| PCA-BPNN     | 88.4  | 11.6  |
| PCA-RRBFNN   | 91.7  | 8.3   |
| PCA-PSO-BPNN | 95.4  | 4.6   |
| 本文           | 99.7  | 0.3   |

4 结束语

本文针对当前复杂的入侵行为, 以及传统的网

络入侵检测效率低下,误报率高,正确率低的情况.提出基于主成分分析、贝叶斯的网络入侵检测模型.首先利用主成分分析进行降维,降低原本数据集的复杂度;再次,使用贝叶斯进行分类,从而判断是否有入侵行为.仿真结果表明,相对于其他的入侵检测模型,本文算法提高了入侵检测的效率,降低了错误率,适合当前的网络入侵检测.未来我们将考虑在不改变贝叶斯的分类效率下,进一步的缩减关键属性,从整体上进一步提高检测效率,同时研究提高 U2R 检测效率,整体上提高本文算法模型的可行性.

#### 参考文献:

- [1] 张然.入侵检测技术研究综述[J].小型微型计算机系统,2003,24(7):1113-1118.
- [2] 饶鲜,董春曦,杨绍全.基于支持向量机的入侵检测系统[J].软件学报,2003,14(4):798-803.
- [3] 焦从信,王崇骏,陈世福.基于完全无向图的贝叶斯分类器在入侵检测中的应用[J].计算机科学,2008,35

(9):83-86.

- [4] LI Shu-jun, CHEN Guan-rong, MOU Xuan-qin. On the security of the Yi-Tan-Siew chaotic cipher[J]. IEEE Trans on Circuits and Systems II: Express Briefs, 2004, 51(12): 665-669.
- [5] 肖海军,洪帆,张昭理,等.基于融合分类和支持向量机的入侵检测研究[J].计算机仿真,2008,25(4):130-132.
- [6] 陈丽丽,李卫,管晓宏,等.一种基于网络的入侵检测系统的研究与实现[J].微电子学与计算机,2004,21(6):63-65.
- [7] KDDCup1999 Data. [EB/OL]. [2013-01-26]. <http://kdd.ics.nci.edu/databases/kddcup99/kddcup99.html>, 1999.

#### 作者简介:

章倩女,(1987-),硕士,研究方向为复杂网络安全.

周健男,(1960-),博士,副教授.研究方向为复杂网络安全.

(上接第 118 页)

- [2] 张学工.关于统计学习理论与支持向量机[J].自动化学报,2000,26(1):32-42.
- [3] 张国云.支持向量机算法及其应用研究[D].长沙:湖南大学,2006.
- [4] Lee Yuh-Jye, O Mangasarian L. SSVM: a smooth support vector machine for classification[J]. Computational optimization and Applications, 2001, 22(1): 5-21.
- [5] 袁玉波.多项式光滑的支撑向量机[J].计算机学报,2005(1):9-17.
- [6] Fan Yanfeng, Zhang Dexian, He Huacan. A new approach for attribute importance measure based on TCA-SSVM[J]. 2009 Global Congress on Intelligent

Systems, Xiamen, 2009(5):481-485

- [7] 熊金志,胡金莲,袁华强,等.一类光滑支持向量机新函数的研究[J].电子学报,2007,35(2):366-370.
- [8] 刘叶青,刘三阳,谷明涛.广义支持向量机的多项式光滑函数法[J].计算机工程与应用,2011,47(33):52-54.

#### 作者简介:

冯咲男,(1964-),硕士,讲师.研究方向为模式识别.

杨志晓男,(1974-),博士,副教授.研究方向为不确定智能理论、技术与应用.

范艳峰女,(1973-),博士,副教授.研究方向为人工智能.