

# 用于入侵检测的基于粗糙集的贝叶斯分类器

翟素兰, 郑 诚

(安徽大学 计算机科学与技术学院, 安徽 合肥 230039)

**摘 要:**网络安全的问题日趋严重,入侵检测的研究是当今的研究热点。将数据挖掘和机器学习技术用于入侵检测是一个可行的方法。有很多算法用于入侵检测中,但有的是正确率比较低,也有的是学习或分类时间长,这些都限制了入侵检测系统在实际中的应用。文中提出了将粗糙集用于网络侦听的海量数据的属性约简,而后提出使用朴素贝叶斯进行分类预测。该方法的准确率高,而且时间性能好,适用于网络入侵检测的要求。

**关键词:**入侵检测;朴素贝叶斯;粗糙集;属性约简

**中图分类号:**TP393.08

**文献标识码:**A

**文章编号:**1005-3751(2006)01-0226-02

## Bayes Classifier Based on Rough Set Used in Intrusion Detection

ZHAI Su-lan, ZHENG Cheng

(School of Computer Science and Technology, Anhui University, Hefei 230039, China)

**Abstract:** The technology of data mining and machine learning has been used in intrusion detection. The algorithm used in IDS needs that the accurate rate is high and the time of learning or classifying is short. Yet, lots of algorithms used in IDS cannot meet the needs which limit the use of IDS in practice. In the paper, the naive bayes classifier based rough set reduction is proposed to use in IDS. The structure of naive bayes is simple, and learning correct efficiency and time efficiency is perfect. But it needs the independence of feature, which can be achieved by reduction based on rough set. It is fit for intrusion detection.

**Key words:** intrusion detection system; naive bayes; rough set; feature reduction

### 0 引言

随着计算机及网络应用的日益广泛深入,计算机系统已经从独立的主机发展到复杂的、互连的开放式系统,这种情况导致计算机及网络的入侵问题越来越突出,为保护系统的安全,需要建立防御入侵机制。入侵检测系统(Intrusion Detection System, IDS)就是监控计算机系统的动态行为特征并据此判断是否有入侵的系统。

目前的入侵检测方法分为两类:异常入侵检测(anomaly intrusion detection)和误用检测(misuse intrusion detection)。异常检测的原理是:根据用户的行为或资源使用状况的正常程度来判断是否为入侵。该方法通用性强,甚至可以检测新的入侵行为,但是对整个系统的正常状态的描述是非常困难的,而且系统状态是动态变化的,所以它主要缺陷在于误检率非常高。误用检测:运用已知攻击方式,根据已定义好的入侵检测模式,通过判断这些入侵模式是否出现来检测。这种方法依据建立入侵特征知识库判断,所以检测准确率高,并且结果显示便于系统处理,及早驱逐入侵。当前的误用检测系统如 IDDES,已知

的入侵模型由专家编码成专家系统规则,利用专家系统匹配已知入侵形式。该系统灵活性高,检测能力大,但是计算代价高,以降低系统的运行速度为代价。一个入侵检测系统应该及时地判断入侵行为。

当前用于入侵检测的算法有关联规则、神经网络、决策树等比较经典的算法。这些算法具有一定的准确性,而且不消耗太多的系统资源,不影响系统的正常运行。但这些算法在使用中多存在这样或那样的不足。文中提出的检测方法是基于粗糙集的朴素贝叶斯算法。研究表明朴素贝叶斯算法的准确率可以和神经网络、决策树相比,而时效性非常高<sup>[1]</sup>,更适用于网络入侵检测。文中首先使用粗糙集对数据进行属性的约简,除去冗余属性,保证属性间的独立性,然后使用朴素贝叶斯分类器进行学习和预测。使用的实验数据是 KDD99 数据集<sup>[2]</sup>。KDD99 数据集是 MIT 的林肯实验室提供的作为 KDD CUP 99 比赛用的,该数据集是模拟美国空军网络环境获得的 9 个星期的 TCP 元数据,这些数据的基础是正常的网络数据,但是其中被人为地添加多种入侵数据,因此数据的分布概率和正常环境的分布概率是不一致的。

### 1 基于粗糙集的属性约简

波兰科学家 Pawlak 提出的 Rough Set 理论是一种处理不精确、不相容和不完全数据的新的数学工具。Rough

收稿日期:2005-04-15

基金项目:安徽省教育厅自然基金资助项目(2002kj009)

作者简介:翟素兰(1977--),女,安徽涡阳人,硕士研究生,研究方向为数据挖掘、网络安全。

Set 理论的基础是定义了一种简单的等价关系,并使用这种等价关系对样本集合划分等价类。粗糙集已广泛地用于数据挖掘,数据约简也是其一个重要的应用领域<sup>[3]</sup>。

定义1 信息系统是一个二元组  $I = (U, A)$ , 其中  $U$  是一个非空的有限对象集,称为对象空间; $A$  是一个非空的属性集,每个属性  $a$  确定了一个从对象空间到  $a$  的值域之间的映射,即对  $a \in A, a: U \rightarrow V_a, V_a$  是属性  $a$  的值域。

在信息系统中,有些属性很重要,相对于其它属性,它们有特殊的地位,这样的属性被特别定义为决策属性,引入决策属性的信息系统就变成了决策系统。

定义2 决策系统是指任何形为  $I = (U, A \cup \{d\})$  的信息系统,这里  $d$  是决策属性,  $A$  为决策系统的条件属性集,  $a \in A$  是条件属性。

定义3 关于决策表的约简 (decision relational reduction) 是指决策系统  $I = (U, A \cup \{d\})$  中,使  $IND_I(D, d) = IND_I(A, d)$  成立的最小属性集  $B$ 。

定义4 设  $R$  是一个等价关系族,  $r \in R$ , 如果  $IND(R) = IND(R - \{r\})$ , 则称  $r$  在  $R$  中是可被约去的知识;如果  $P = R - \{r\}$  是独立的,则称  $P$  是  $R$  的一个约简。

A. Skowron 于 1991 年提出了一种用分明矩阵表示知识的方法<sup>[3]</sup>,该方法便于解释和计算数据和约简。他也提出利用分明矩阵进行属性约简的方法。

定义5 设  $B \in RED(S)$ , 则约简  $B$  中的所有属性都是相互独立的,即对任意  $a, a' \in B$  且  $a \neq a'$ , 既没有  $|a| \rightarrow |a'|$  成立,也没有  $|a'| \rightarrow |a|$  成立。

该定义表明,约简中的每个属性都是独立的,它不与任何属性相关。

## 2 朴素贝叶斯分类器

朴素贝叶斯分类器 (Naive Bayes Classifier, NBC) 是贝叶斯学习方法中实用性很高的分类器<sup>[1]</sup>。在某些领域内其性能可以与神经网络和决策树学习相当<sup>[4]</sup>。下面介绍朴素贝叶斯分类器的相关概念。

贝叶斯公式:

$$\begin{aligned} h_{MAP} &= \arg \max_{h \in H} P(h | D) \\ &= \arg \max_{h \in H} \frac{p(D | h) p(h)}{p(D)} \\ &= \arg \max_{h \in H} p(D | h) p(h) \end{aligned}$$

式中,  $p(h)$  为假设  $h$  的先验概率;  $p(D | h)$  代表假设  $h$  成立时观察到的  $h$  的概率;  $p(h | D)$  为给定训练数据  $D$  时  $h$  成立的概率,这是我们关心的。这里需要的是给定数据  $D$  时可能性最大的假设,也就是极大后验 (maximum a posterior, MAP) 假设。

NBC 将训练实例以及新实例表示为  $(a_1, a_2, \dots, a_n, v_j)$ , 其中  $a_i$  是条件属性,  $v_j$  为目标值,对应数据中的每一类,它们彼此独立,具有完备性。NBC 基于一个这样的简单假设:在给定目标值时,条件属性值之间相互条件独立。

也就是说,在给定目标值情况下,观察到联合的  $a_1, a_2, \dots, a_n$  的概率等于每个单独属性的概率乘积:

$$P(a_1, a_2, \dots, a_n | v_j) = \prod_{i=1}^n p(a_i | v_j)$$

将其带入贝叶斯公式,得到 NBC 所使用到的方法:

$$v_{NB} = \arg \max P(v_j) \prod_{i=1}^n p(a_i | v_j)$$

事实上,在很多领域当违背了这种独立性的假设时, NBC 也表现出了相当的健壮性和高效性<sup>[4]</sup>。

## 3 实验与分析

文中在 KDD99 数据集上设计实现了朴素贝叶斯算法的效率和效果的实验。试验数据有 494 020 条,共有 23 类,把这些类网络行为映射到 5 大类网络行为中。KDD99 数据集有 41 个属性,其中 34 个为数值型变量,7 个为符号变量。

在实验中,实验数据采用比较均匀的抽样方式进行抽样,组成 Rough Set 的学习数据集。在 5 类网络行为中,从 normal 类和 dos 类中抽取了 3% 的记录,而在 probe 和 R2L 中抽取了 10% 的记录,对于 U2R 抽取了一半的记录(该类在训练数据集中共有 52 条记录)。采用这种方式共组成 5 组学习数据集,并对其中的连续属性进行了无监督的离散化,也就是将属性离散化到 10 个等宽的区间内,然后进行 Rough Set 的学习。试验选用波兰的 Rosetta 软件<sup>[5]</sup>。该软件采用的基于差别矩阵用于属性和信息表的约简。考察属性对目标分类的相对重要性,删除冗余属性。从众多约简属性结果里,根据所掌握到的网络连接的背景知识,最终使用的条件属性有 service(网络服务), flag(连接状态), src\_bytes(源主机到目的主机的字节数), dst\_bytes(目的主机到源主机的字节数), dst\_host\_srv\_count, diff\_srv\_rate(不同服务连接占的百分比)。

然后使用朴素贝叶斯分类器进行了分类学习和预测,将结果同经典的机器学习算法决策树 C4.5 的效果做了比较,即 NBC 与 C4.5 在入侵检测中性能的比较(见表 1)。

表 1 NBC 与 C4.5 在入侵检测中性能的比较

学习样本集	样本 1	样本 2	样本 3	样本 4	样本 5	样本 6	样本 7	样本 8	样本 9	样本 10	平均
NBC 的分类准确率(%)	98.3	97.9	98.1	97.5	98.0	98.2	98.1	98.6	98.7	97.5	98.09
NBC 学习用时(s)	2.1	2.0	2.1	2.1	2.1	2.1	2.0	2.0	2.1	2.0	2.06
NBC 分类用时(s)	5.5	3.8	3.1	3.4	3.7	4.0	4.0	3.4	3.4	3.5	3.78
C4.5 的分类准确率(%)	98.1	96.8	97.2	96.7	96.9	97.2	97.0	97.3	96.5	98.0	97.17
C4.5 的学习用时(s)	7.1	8.2	8.0	8.2	8.3	7.8	7.3	9.0	8.1	8.1	8.01
C4.5 分类用时(s)	13.0	14.1	11.9	11.1	12.0	14.3	13.0	12.1	11.8	13.1	12.64

(下转第 230 页)

### 3.2.4 集成到应用服务器

最后需要把整个认证模块集成到应用服务器中去。目前在应用服务器市场中的 JAAS 产品还不是很一致,使用 JAAS 的 J2EE 应用服务器有一些细微的差别。例如 JBoss 使用自己的结构,将 JAAS 集成到了一个更大的安全框架中;而虽然 WebLogic 也使用了 JAAS,安全框架却完全不一样。在文中所涉及的应用中,使用的是 Tomcat 5。部署在该服务器中的应用程序需要在它的部署描述文件中增加<Realm>元素的定义:

```
<? xml version = '1.0' encoding = 'utf-8'? >
<Context docBase = "d:/captcha - login/web" path = "/login" debug = "9">
< Realm className = "org.apache.catalina.realm.JAASRealm"
appName = "clogin" debug = "99" roleClassNames = "ww.jaas.CPrincipal"
userClassNames = "ww.jaas.CPrincipal"/>
</Context>
```

将认证模块插入到应用中去,仅仅需要的是一个配置文件,如下代码段所示:

```
clogin|ww.jaas.Clogin Module required debug = true;
};//JAAS 配置文件:jaas.config
```

### 3.2.5 新的认证模块的实际应用

在一个基于 J2EE 平台的房地产交易系统中,使用了该认证模块,有效防止了机器自动登录,阻止了垃圾信息的发布,增强了安全性。其运行效果如图 2 所示。

## 4 结束语

为避免人为利用自动填表程序反复登录或发表垃圾信息,许多基于 J2EE 平台的网络应用系统必须区分是真正的人还是自动填表程序在操作。CAPTCHA 能够在人和自动填表程序之间作出判断。在文中,介绍了 CAPTCHA 的相关概念,并对 J2EE 中安全策略和 Java 认

证和授权服务作了一些阐述;最后在这些概念基础上,用 CAPTCHA 扩展了 JAAS 中的登录模块,并把这个模块集成到应用服务器中。由于上述实现过程是建立在标准 J2EE 安全机制上,所以可以在任何 J2EE 应用上复用。

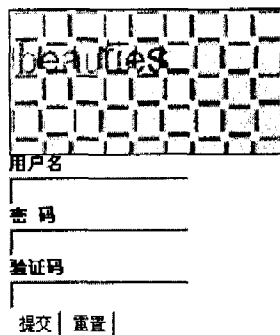


图 2 运行效果

### 参考文献:

- [1] 王 敏,吉 逸. Java2 环境下身份认证和授权机制的研究[J]. 微机发展,2003,13(5): 40-42.
- [2] 赵仲孟,沈海斌. J2EE 应用服务器安全服务体系的分析与实现[J]. 计算机工程与应用,2003,39(21): 175-177.
- [3] Sun Microsystems. Java™ Authentication and Authorization Service (JAAS) LoginModule Developer's Guide[EB/OL]. <http://java.sun.com/j2se/1.4.2/docs/guide/security/jaas/JAASRefGuide.html>,2001.
- [4] Sun Microsystems. Java™ Authentication and Authorization Service (JAAS) Reference Guide for the Java2 SDK, Standard Edition[EB/OL]. <http://java.sun.com/j2se/1.4.2/docs/guide/security/jaas/JAASLMDevGuide.html>,2001.
- [5] von Ahn L, Blum M, Hopper N J, et al. CAPTCHA: Using Hard AI Problems For Security[J]. Lecture Notes in Computer Science, 2003, 2656(9): 294-311.

(上接第 227 页)

分析表 1 中 NBC 与 C4.5 在入侵检测中性能的比较,可以看出朴素贝叶斯分类器的准确率同决策树的准确率相当,但其无论是学习还是分类时间都明显低于 C4.5 的时间。这是因为,朴素贝叶斯的属性独立的假设简化了运算。由于在入侵检测系统中,不仅要求能准确地检测出入侵行为,而且还需要快速检测出入侵行为,这样才可能及时采取措施,降低或消除入侵行为对系统造成的破坏。通过实验可以证实朴素贝叶斯分类器可以满足入侵检测的这种要求。由于朴素贝叶斯分类器的前提是属性的严格独立,在众多的约简算法中,基于粗糙集的约简可以实现这种约简。

但是由于朴素贝叶斯分类器的理论基础是贝叶斯法则,当测试数据同训练数据的概率分布出现比较大的差异时,朴素贝叶斯分类器的准确率会受到严重影响。所以将朴素贝叶斯分类器用于网络入侵检测系统,要求经常更新

训练数据,保证训练数据与网络的实时环境中的网络行为具有基本一致的概率分布。

### 参考文献:

- [1] Mitchell T M. 机器学习[M]. 曾华军,张银奎,等译. 北京:机械工业出版社,2003.
- [2] Information and Computer Science University of California, Irvine. KDD cup 1999 Data[EB/OL]. <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>,1999-10.
- [3] 刘 清. Rough 集及 Rough 推理[M]. 北京:科学出版社,2001.
- [4] 史忠植. 知识发现[M]. 北京:清华大学出版社,2002.
- [5] Knowledge Systems Group, Dept. of Computer and Information Science, Norwegian University of Science and Technology, Trondheim, Norway. ROSETTA[EB/OL]. <http://rosetta.lcb.uu.se/general/download/1999>.