基于半监督学习的入侵检测系统

戴 林,姜 梅
(青岛理工大学 计算机工程学院,山东 青岛 266033)

摘 要:在入侵检测方法中,半监督学习作为一种特殊的学习形式,结合了监督学习与非监督学习在检测已知模式数据与未知模式数据方面各自的优点。据此,为进一步提高入侵检测系统的检测准确性,提出一种结合SVM与KMO(online k-means)算法各自优点的半监督入侵检测模型。该模型首先利用SVM算法对全部的输入数据进行区分,然后将其认为的合法数据集用KMO算法分类,以该结果作为决策模块的输入并做出最终的响应。实验显示,文中模型比单独使用其中的任一种方法具有更高的检测准确率。由此可见,该模型对于实际的入侵检测系统具有实用价值。

关键词:半监督学习;入侵检测;SVM;KMO;统计学习
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2011)01-0162-03

Semi-Supervised Learning-Based Network Intrusion Detection System

DAI Lin, JIANG Mei
(College of Computer Engineering, Qingdao Technological University, Qingdao 266033, China)

Abstract: In the intrusion detection method, semi-supervised learning as a special form of learning, combines the advantages of supervised learning and unsupervised learning in detecting the known and unknown mode of data. Accordingly, to improve the detection accuracy, proposed a semi-supervised intrusion detection model that integrates the respective advantages of SVM and KMO (online k-means). In this model, firstly use the SVM algorithm to filter all the input data, then the considered legitimate data is classified with KMO, so the decision-making module can respond the final input data. Experiments show that the model has a higher detection accuracy than use each of them alone. Thus, the model has practical value for real intrusion detection system.

Key words: semi-supervised learning; intrusion detection; SVM; KMO; statistical learning

0 引 言

入侵检测(Intrusion Detection)是通过收集和分析网络行为、安全日志、审计数据、其它网络上可以获得的信息以及计算机系统中若干关键点的信息,来检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。其目标是以较高的检测率和以较低的错误报警率来检测入侵。

具有入侵检测功能的系统称为入侵检测系统(IDS, Intrusion Detection System)。基于不同的学习方法,IDS常被分类为基于监督学习的IDS和基于非监督学习[1-3]的IDS。前者特点是对已知的模式有较高的正确识别率,而对未知模式的攻击识别率较低。后者则恰好相反,对未知模式的入侵识别率通常比前者高,但由于其未经过相应的训练,对已知模式的入侵检测率通常低于相应的监督学习方法。

收稿日期:2010-04-18;**修回日期**:2010-07-08
作者简介:戴 林(1985-),男,山东青岛人,硕士研究生,研究方向为信息安全;姜 梅,博士,副教授,研究方向为入侵检测与网络安全。

1 半监督分类理论

半监督分类[4,5]是分类的一种特殊形式。传统的分类器只使用标记数据(特征/标签对)来训练。然而通常获得标记实例要花费大量的时间,并且很难获得,因为它们需要大量有经验注释者的努力。相反,非标记数据可以相对容易的收集,但是很难使用它们。半监督学习通过标记的数据与大量未标记数据一起来解决这个问题,来建立更好的分类器。由于半监督学习需要更少的人工努力而且有更高的入侵检测率,所以无论在理论还是实践上都很有价值。

1.1 SVM理论

支持向量机(Support Vector Machine, SVM)是基于统计学习理论的一种模式识别技术[6,7]。SVM的核心思想是:用事先选择的非线性映射变换(即核函数)将输入向量映射到高维空间中,然后在高维空间中构造最优分类超平面,如图1所示。

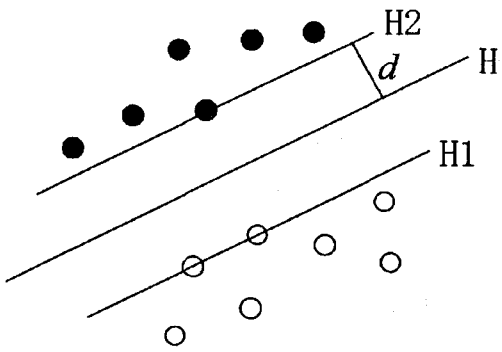

图 1　最优分类面是以最大间隔将数据分开的超平面

图 1 中,空心圆与实心圆分别代表不同类型的样本,H 为最优分类面,$H1$、$H2$ 分别为过各类中离分类面最近的样本且平行于分类面的面,它们之间的距离叫做分类间隔。所谓最优分类面就是要求分类面不但能将两类样本正确分开,而且还使分类间隔最大。分类面方程为 $w \cdot x + b = 0$,对它进行归一化,使得对现行可分的样本集 (x_i, y_i), $i = 1, \cdots, m$, $x \in R^N$, $y \in \{+1, -1\}$,满足 $y_i[(w \cdot x) + b] - 1 \geq 0$, $i = 1, \cdots, m$。此时分类间隔等于 $\frac{2}{\| W \|}$,使间隔最大等价于使 $\| W \|^2$ 最小,满足上式且使 $\frac{\| W \|^2}{2}$ 最小的分类面就是最优分类面,$H1$、$H2$ 上的训练样本点称作支持向量(Support Vectors),除非特殊指定,$\| \cdot \|$ 代表 $L2$ 范式。

1.2　KMO 算法

广泛使用的标准 k-means 算法[8~10]最小化了均方误差目标函数:

$$E = \frac{1}{N} \sum_{n} \| x_n - \mu_{y_n} \|^2$$

其中 $y_n = \arg\min_k \| x_n - \mu_{y_n} \|^2$ 是数据向量 x_n 的聚类特征,μ_{y_n} 是簇 y_n 的质心。K 均值算法的流行很大程度上归功于它的简洁性、较低的时间复杂性和较快的收敛速度。文中给出 k - means 算法的一种联机形式,KMO 算法(online k - means algorithm)。

算法:联机 K 均值算法(KMO)

输入:IR^d 维空间中的 N 个数据向量 $X = \{x_1, \cdots, x_N\}$ 的集合以及聚类的数量 K。

输出:通过给定的聚类特征向量 $Y = \{y_1, \cdots, y_N\}$, $y_N \in \{1, \cdots, K\}$,得出数据向量的一个划分。

步骤 1:初始化:初始化类质心向量 $\{\mu_1, \cdots, \mu_K\}$;

步骤 2:循环迭代 M 次

对于每一个数据向量 x_N,设置 $y_n = \arg\min_k \| x_n - \mu_{y_n} \|^2$,然后更新质心 μ_{y_n} 为:

$$\mu_{y_n}^{(new)} = \mu_{y_n} - \frac{\partial E}{\partial \mu_{y_n}} = \mu_{y_n} + \xi(x_n - \mu_{y_n})$$

其中 ξ 是一个学习速率参数,它经常被设置为一个较小的正数(例如,0.05)。

这个数字也可以在学习过程中逐渐递减。

2　入侵检测系统模型

基于半监督的网络入侵检测系统主要由数据采集、网络数据预处理、入侵检测决策系统以及决策响应 4 部分组成,其中入侵检测决策系统中包含了 SVM 分类器以及 KMO 算法。整个系统的功能框架结构如图 2 所示。

该框架的思想是用 SVM 来过滤已知模式的攻击,过滤后的样本作为 KMO 算法的输入,用它来检测未知模式的攻击。从图中可以看出,KMO 算法单元无需接受预先的样本训练,因为它是一种非监督的聚类算法。

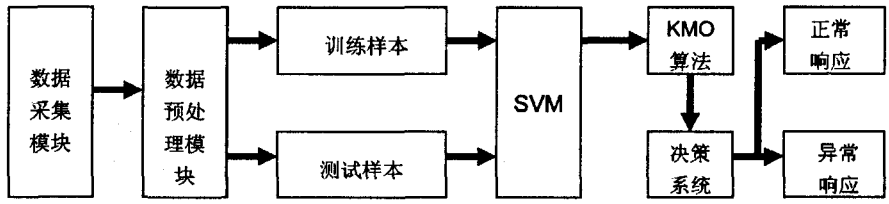

图 2　基于半监督学习的入侵检测系统框架

3　实验及数据分析

文中所有实验运行于 Pentium4 3.0GHz CPU、512MB RAM 的 PC 机上,操作系统为 Window XP SP3,实验工具为 MATLAB 以及 lib-svm。实验数据采用 KDD CUP 1999 中的 corrected 数据集[11,12],它包含 311029 条记录,其中正常数据及各种攻击数据所占的比例如表 1 所示。

表 1　各种实验数据所占比例

攻击类别	Normal	DoS	U2R	R2L	Probe	总计
包含的攻击类型	0	10	10	11	6	37
数量	60593	229853	2636	13781	4166	311029
所占百分比	19.48	73.90	0.85	4.43	1.34	100

值得一提的是,训练集的构建对于分类器的分类时间和效果具有很大的影响。因此文中采用基于主成分分析的方法将其降维,选择第 42 维以及前 41 维特征中的 14 维作为样本特征,并使用文献[13]和[14]中的方法来标准化数据。由于原始数据集中的数据量较大,在此随机抽取实验数据集中 10% 的 normal 数据以及 10% 的 DoS 攻击数据作为 SVM 的训练数据。将全部的 U2R、R2L、Probe 数据和随机抽取的 20% normal

以及20% DoS数据用作测试数据。实验重复5次,图3为各次实验所需时间,表2中的数据均为5次实验的均值。

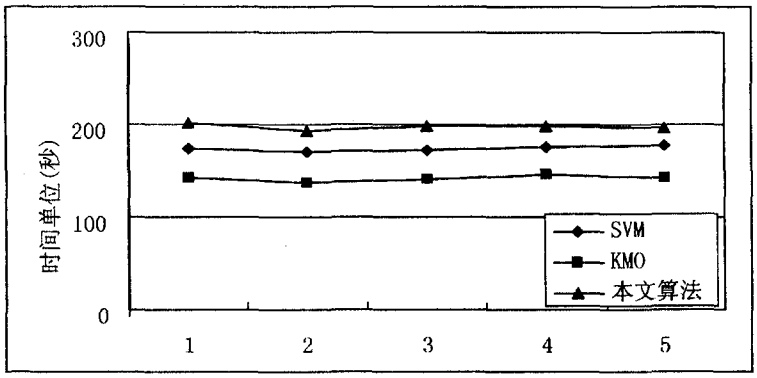

图3 各种算法的时间耗费比较

表2 不同分类方式在Corrected数据集上的结果比较

		检测精度(%)				
		DoS	U2R	R2L	Probe	总体
假阳性率	SVM	94.49	0	27.10	65.38	75.24
	KMO	70.17	53.81	5.79	94.06	74.39
(fpr)=5%	本文模型	75.91	53.81	21.37	87.63	78.96
假阳性率	SVM	94.51	0	27.93	66.02	75.59
	KMO	70.43	92.36	73.54	94.07	82.76
(fpr)=10%	本文模型	75.92	92.36	72.18	87.89	86.83
假阳性率	SVM	94.51	0	28.64	66.83	75.64
	KMO	70.46	97.39	81.92	95.12	85.74
(fpr)=15%	本文模型	75.92	97.39	83.29	88.02	89.31

从表2中可以看出:SVM对于在训练集中所出现的DoS攻击具有较高的检测率。对于R2L类型的攻击,在fpr为5%时优于KMO算法,在fpr分别为10%、15%时不及KMO。而KMO算法虽然对DoS的检测率比SVM低,但是它对未知模式的攻击类别(在SVM的训练集中未出现)比SVM有更高的检测正确率。除DoS类型的攻击,文中所提出的模型均比SVM有更高的检测正确率,而且其总体正确率也比单独使用任一种分类器要好。实验结果表明,文中所提出的模型是可行的。

4 结束语

文中主要提出了一种基于半监督学习的入侵检测模型,并通过实验验证了它在入侵检测中的可行性和有效性。从实验数据中可以看出,文中提出的模型融合了SVM与KMO算法的优点。但是,在检测时间上却比单独使用SVM要长。因此,该模型还需进一步改进。作为未来的方向,还需对如何提高检测DoS类型攻击的正确率及如何缩短检测时间做进一步的研究。

参考文献:

[1] Portnoy L,Eskin E,Stolfo S. Intrusion detection with unlabeled data using clustering[C]//In ACM Workshop on Data Mining Applied to Security. Philadelphia,PA:[s. n.],2001.

[2] Eskin E,Arnold A,Preau M,et al. A geometric framework for unsupervised anomaly detection:detecting intrusions in unlabeled data[R]. New York:Department of Computer Science,Columbia University,2007.

[3] 肖竟华,卢 娜. 基于网络的入侵检测系统的研究及实现[J]. 计算机技术与发展,2007,17(2):242-244.

[4] 杨晓强. 一种进化半监督式模糊聚类的入侵检测算法[J]. 计算机工程与应用,2008,44(4):33-35.

[5] ZHU Xiaojin. Semi-supervised learning literature survey[EB/OL]. 2009-09. http://pages.cs.wisc.edu/? jerryzhu/research/ssl/semireview.html.

[6] Chapelle O. Training a Support Vector Machine in the Primal[J]. Neural Computation,2007,19(5):1155-1178.

[7] 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):798-802.

[8] 郭文普,孙继银,仟 俊. 一种基于数据融合的分布式入侵检测系统[J]. 计算机技术与发展,2006,16(2):217-219.

[9] LI W,ZHANG K,LI B,et al. An efficient framework for intrusion detection based on data mining[C]//In Proceedings 2005 ICSC Congress on Computational Intelligence Methods and Applications. [s. l.]:IEEE Computer Society,2005.

[10] 程玉青,梅登华,陈龙飞. 基于数据挖掘的入侵检测系统模型[J]. 计算机技术与发展,2009,19(12):123-126.

[11] KDD-99 dataset[EB/OL]. 2009-01-09. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[12] Elakn C. Results of the KDD'99 classifier learning[EB/OL]. 2009-01-09. ACM SIGKDD,2000.

[13] 朱永宣. 基于模式识别的入侵检测关键技术研究[D]. 北京:北京邮电大学,2006.

[14] 毛 勇. 基于支持向量机的特征选择方法的研究与应用[D]. 杭州:浙江大学,2006.