基于粗糙集-支持向量机理论的过滤误报警方法

肖　云[①②]　韩崇昭[①]　郑庆华[①]　赵　婷[①]
[①](西安交通大学电子与信息工程学院　西安 710049)
[②](西北大学信息科学与技术学院　西安 710127)

摘　要：为过滤入侵检测系统报警数据中的误报警，根据报警的根源性和时间性总结出了区分真报警和误报警的19 个相关属性，并提出了一种基于粗糙集-支持向量机理论的过滤误报警的方法。该方法首先采用粗糙集理论去除相关属性中的冗余属性，然后将具有约简后的 10 个属性的报警数据集上的误报警过滤问题转化为分类问题，采用支持向量机理论构造分类器以过滤误报警。实验采用由网络入侵检测器 Snort 监控美国国防部高级研究计划局 1999 年入侵评测数据(DARPA99)产生的报警数据，结果表明提出的方法在漏报警约增加 1.6%的代价下，可过滤掉约98%的误报警。该结果优于文献中使用相同数据、相同入侵检测系统的其它方法的结果。

关键词：入侵检测；误报警；漏报警；粗糙集；支持向量机
中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1009-5896(2007)12-3011-04

An Approach to Filter False Positive Alerts Based on RS-SVM Theory

Xiao Yun[①②]　Han Chong-zhao[①]　Zheng Qing-hua[①]　Zhao ting[①]
[①](*School of Electronic & Information Engineering*, *Xi'an Jiaotong University*, *Xi'an* 710049, *China*)
[②](*School of Information Science and Technology*, *Northwest University*, *Xi'an* 710127, *China*)

Abstract: To filter false positive alerts generated by Intrusion Detection Systems (IDS), 19 related attributes for distinguishing false positive alerts from true alerts are summarized according to the root and timeliness of intrusion alerts, and an approach to filter these false positive alerts based on RS-SVM (Rough Set and Support Vector Machine) theory is proposed. First, redundant attributes are removed and 10 attributes are obtained utilizing rough set theory in the proposed approach. Then the problem of filtering false positive alerts on the dataset with those 10 attributes is transformed to classification problem, and the classifier is constructed using support vector machine theory. The experimental data is the alert dataset raised by Snort, a network intrusion detection system, monitoring the Defense Advanced Research Projects Agency 1999 intrusion evaluation data (DARPA99). The experimental results show that the proposed approach can reduce about 98% false positive alerts at the cost of increasing about 1.6% false negative alerts. The results of this method are better than those of the other methods that adopt the same dataset and same IDS reported in the literature.

Key words: Intrusion detection; False positive alert; False negative alert; Rough Set (RS); Support Vector Machine (SVM)

1　引言

入侵检测系统(Intrusion Detection System，IDS)是对计算机或计算机网络系统中的攻击行为进行检测的自动系统。实际中运行的IDS均存在着大量的误报警，据统计误报警的数量最高可达 99%[1]，这使得人类分析员难以快速而准确地识别出真正与攻击有关的报警(以下简称为真报警)。误报警产生的原因可以分为两类：第一类是攻击特征描述不完善或者检测系统自身在算法和分析方法等方面存在缺陷；第二类是网络数据包内确实包含攻击特征，但是对于具体的目标或者环境没有作用或不够成威胁，仍被判定为攻击的情况。事实上，由于报警被误判后的代价是不均衡的，即真报警被误判为误报警所付出的代价要比相反的大，因此如何在保证较高的检测率和较低的误报率的前提下降低IDS的误报警已经成为入侵检测领域的研究热点。本文在前人研究的基础上提出一种基于粗糙集-支持向量机(RS-SVM)理论的过滤误报警方法，采用网络入侵检测器Snort在DARPA99 入侵评测数据集上产生报警数据集，取得了较好的实验结果。

2006-05-25 收到，2006-10-24 改回
国家 863 计划项目(2004AA1Z2280)和国家 973 发展规划项目(2001CB309403)资助课题

2　相关工作

目前，研究者已经在降低IDS误报警方面做出了一定的研究成果。Manganaris等人通过分析报警流来发现关联规则，并提出一个过滤误报警的框架[2]。Wang等人通过对黑客行为进行分析，得出了与误报警相关的7个属性，然后使用3种基于数据挖掘和统计模型的方法估计误报警发生的可能

性，以降低误报警[3]。Alharby等人使用连续和离散序列模式来降低误报警[4]。数据挖掘技术也被用来降低IDS中的误报警，该方法通过建立一个误报警的分类模型来降低网络入侵检测系统的误报警[5]。Pietraszek采用RIPPER规则建立真报警和误报警的分类器，开发出了一个降低误报警的原型系统ALAC(Adaptive Learner for Alert Classification)，能够显著降低误报警[6]。Zhang等人使用文本分类的方法抑制入侵检测的误报警[7]。异常检测的思想也被应用于降低IDS的误报警，即通过对IDS的正常报警模式进行建模，使用最近邻法(KNN)构造分类器对输入的报警进行异常检测[8]。

上述降低入侵检测系统的误报警的方法各有利弊：若具有很强的专业知识，则存在方法上的欠缺[2, 3]；若利用高效的智能方法，则较少利用专业知识[4~8]。因此，有必要充分利用专业知识并采取高效的智能方法，以便更好地解决IDS的高误报警的难题。本文在前人研究的基础上，总结出了区分真报警和误报警的一系列属性，并利用粗糙集理论对这些属性进行约简，将具有约简后属性的数据集上的过滤误报警的问题转化为数据分类问题，采用高效的支持向量机构造分类器，并对方法的性能进行了测试。

3 基于粗糙集-支持向量机(RS-SVM)理论的过滤误报警方法

3.1 报警属性

IDS 的原始报警数据包含着丰富的信息，本文对之进行文本解析，统一成如下所示的六元组：

Alert=<Alert-ID，Attack-Time，Attack-Name，Source-IP，Destination-IP，Vulnerability > 其中 Alert-ID 代表报警的编号；Attack-Time 报警发生的时间；Attack-Name 是攻击名称；Source-IP 是报警中的源 IP 地址；Destination -IP 是报警中的目的 IP 地址； Vulnerability 是攻击所利用的漏洞。

定义 1 根源性报警属性 从报警发生的根源的角度出发，以分析黑客的攻击行为来获取的报警属性。

定义 2 时间性报警属性 从报警发生的时间的角度出发，以调整时间窗的大小来获取的报警属性。

本文在 Wang 和 Pietraszek 研究的基础上，综合根源性报警属性和时间性报警属性，总结出了区分真报警和误报警的 19 个相关的属性，既弥补了 Wang 等人过多的考虑根源性报警属性而忽略了时间性报警属性的不足，又改正了 Pietraszek 仅仅考虑时间性报警属性而较少考虑根源性报警属性的缺陷，具体描述如下：

(1) IP 地址的分类属性：Source-IP-Class，Destination-IP-Class。

将源 IP 和目的 IP 的按照不同的子网进行分类，即分为外网、内网、非军事区(DMZ)。

(2) 黑客行为的时段属性：Source-IP-Timing-Regularity，Destination-IP-Timing-Regularity。

即将一天 24 小时分成 4 个时间段，上午：6:00~12:00，下午：12:00~18:00，前半夜：18:00~24:00，后半夜：24:00~6:00。Source-IP-Timing-Regularity 的值为一天中和当前报警同源 IP 且同时间段的报警数目与和当前报警同源 IP 的报警数目之比，Destination-IP-Timing-Regularity 的值为一天中和当前报警同目的 IP 且同时间段的报警数目与和当前报警同目的 IP 的报警数目之比。

(3) 1，5，30min 内同源 IP 攻击属性：Same-Source-IP-1，Same-Source-IP-5，Same-Source-IP-30。

即从当前报警发生的时间起，以前一段时间内(1，5，30min)和当前报警同源 IP 的报警数目与该段时间内报警总数之比。

(4) 1，5，30min 内同目的 IP 攻击属性：Same-Destinati-on-IP-1， Same-Destination-IP-5，Same -Destination-IP-30。

即从当前报警发生的时间起，以前一段时间内(1，5，30min)和当前报警同目的 IP 的报警数目与该段时间内报警总数之比。

(5) 1，5，30min 内同种攻击属性：Same-Attack-Name-1，Same-Attack-Name-5，Same-Attack-Name-3。

即从当前报警发生的时间起，以前一段时间内(1，5，30min)与当前报警同源 IP 且同攻击名称的报警数目与该段时间内同源 IP 的报警数目之比。

(6) 1，5，30min 内同种漏洞属性：Same-Vulnerability-1，Same-Vulnerability-5，Same-Vulnerability-30。

即从当前报警发生的时间起，以前一段时间内(1，5，30min)和当前报警同目的 IP 且同漏洞的报警数目与该段时间内同目的 IP 的报警数目之比。

(7) 1，5，30min 黑客行为的攻击阶段属性：Prophase-Attack-Name-1 ， Prophase-Attack-Name-5 ， Prophase-Attack-Name-30。

一般可将黑客的攻击分为 4 个阶段：扫描，漏洞探测，权限提升或者拒绝服务攻击，窃取。Prophase-Attack-Name-1 ， Prophase-Attack-Name-5 ， Prophase-Attack-Name-30 的值为从当前报警发生的时间起，以前一段时间内(1，5，30min)在当前报警攻击阶段之前的且同目的 IP 的报警数目与该段时间内同目的 IP 的报警数目之比。

根据以上的定义，可将六元组格式的报警数据集转化成用 19 个属性所表示的用于属性约简和分类的新数据集。在不致引起混淆的情况下，新数据集仍被称为报警数据集。

3.2 粗糙集理论及报警属性约简

粗糙集理论是由Pawlak教授提出的一种小样本学习方法，能够在样本数据集中寻找和发现数据属性之间关系的方法[9]。属性约简是粗糙集理论的核心内容之一，属性约简就是在保持知识库分类能力不变的条件下，删除其中不相关或不重要的属性(相关知识详见文献[9])。本文根据专业知识给出了19个属性，这些属性中可能存在冗余属性。而粗糙集理论的属性约简功能可从所有的属性中筛选出能反映数据之

间本质关系的重要属性。本文将这19个属性作为条件属性，利用上述概念和方法对之进行约简，可得到最小属性集，使用基于最小属性集构成的报警数据进行分类，可提高支持向量机的处理效率。

3.3　支持向量机理论与报警分类

1963年Vapnik在解决模式识别问题时提出了支持向量方法，这种方法从训练集中选择一组特征子集，使得对特征子集的划分等价于对整个数据集的划分，这组特征子集就被称为支持向量(Support Vector，SV)，这种理论称为支持向量机理论[10](相关知识详见文献[10])。根据约简后的属性，本文将每条报警数据转化为一个向量，并根据一定的方法标定出真报警和误报警。此时报警数据集上的误报警过滤问题，可通过应用支持向量机理论构造分类器来解决。即利用标定的训练数据得到支持向量机的训练模型，并使用标定的测试数据进行分类(测试数据的标定结果只用来验证分类的效果)，从而达到过滤误报警的目的。

3.4 基于粗糙集-支持向量机(RS-SVM)理论的过滤误报警方法

基于 RS-SVM 理论的过滤误报警的步骤如下：

(1)样本预处理　对原始的报警数据中进行文本解析，将其表示成 3.1 节所示的六元组格式。

(2)属性获取　对六元组格式的报警数据进行统计，获得每条报警的 19 个属性值，形成待处理的数据集 $D_{\mathrm{RS\_SVM}}$。

(3)属性约简　对数据集 $D_{\mathrm{RS\_SVM}}$ 随机抽取 10%形成用于数据集 D_{RST}，利用粗糙集理论的属性约简的概念和方法对 D_{RST} 进行属性约简，得到一系列的约简属性集；

(4)产生新属性集　结合网络安全的专业知识，选择一组符合要求的新属性集；

(5)归一化处理　按照新属性集及相应的原始数据集 D_{RST} 形成新的数据集 D_{SVM}，并对属性做归一化处理，即 $x_i' = x_i/(\max(x_i)-\min(x_i))$，其中 x_i' 代表归一化后的属性值，x_i 代表归一化前的属性值，$\max(x_i)$ 代表第 i 个属性最大值，$\min(x_i)$ 代表第 i 个属性最小值。

(6)建立 SVM 分类器　从 D_{SVM} 随机抽取 20%的数据形成训练样本集 $D_{\mathrm{SVM\_Tr}}$，选用 RBF 核函数并采用序列最小优化算法(Sequential Minimal Optimization, SMO)来训练 SVM 分类器；

(7)分类　用得到的 SVM 分类器对 D_{SVM} 中其余 80%的数据形成的测试样本集 $D_{\mathrm{SVM\_Te}}$ 进行分类，并输出分类结果。

(8)计算性能指标　真报警率，误报减少率和漏报增加率，计算方法如下：

真报警率 TP＝标定的真报警被检测为真报警的样本数目/标定的真报警样本数目；

误报减少率 DFP＝标定的误报警被检测为误报警的样本数目/标定的误报警样本数目；

漏报增加率 IFP ＝标定的真报警被检测为误报警的样本数目/标定的真报警样本数目。

分析文献[6]中 TP 和 DFP 的 ROC 曲线图，可得 TP 和 DFP 基本成正比例关系，与 IFP 成反比例关系。另外随着分类器分类能力的增强，TP 和 DFP 呈增加趋势，而 IFP 呈减少趋势，与文献[6]所得的结论吻合。

定期检查分类器的分类精度，如果分类精度低于用户定义的阈值，就在旧的训练样本中随机抽取 30%，并与新收集的训练样本一起用于更新训练模型，以保证分类器的分类精度要求。基于 RS-SVM 的误报警过滤系统的框架如图 1 所示。

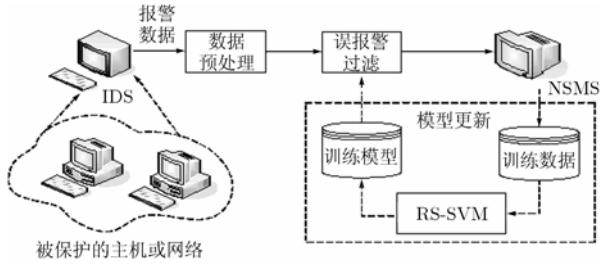

图 1　基于 RS-SVM 的误报警过滤系统的框架

4　实验结果

为验证基于粗糙集-支持向量机理论的过滤误报警方法，实验选用的原始网络流量数据是 1999 年美国国防部高级研究计划局(DARPA)入侵检测评测数据(简称 DARPA99)。本文使用 Snort 产生报警数据作为实验数据，并根据 MIT 林肯实验室提供的 DARPA99 数据的评估结果对之进行标定。本文所采用的粗糙集分析软件是由挪威科技大学计算机和信息科学系的知识系统研究小组开发的软件包 ROSSETA，支持向量机软件采用 libSVM 软件，并选用径向基核函数(RBF)。

原始 DARPA99 数据中第 1、2、3 周的数据为训练数据，第 4、5 周的数据为测试数据，所以本文利用这两个数据集分别使用 Snort 产生报警数据集 DATA1 和 DATA2。DARPA99 中第 1 周和第 3 周的原始数据不包含攻击数据，但是在使用 Snort 监控时仍然产生了多条报警数据，显然这些报警数据就是误报警。报警数据集 DATA1 共 78748 条数据，经过标定后只有 2659 条真报警；数据集 DATA2 共 16115 条数据，标定后只有 2473 条真报警。对两个报警数据集进行文本解析，并从数据集 DATA1 中随机地抽取 10%形成 D_{RST}；利用 ROSSETA 软件进行属性约简，并取其中一组统计属性值相对较为简单的属性集：Destination-IP-Class，Source-IP-Timing-Regularity,Destination-IP-Timing-Regularity，Same-Source-IP-1，Same -Source-IP-5，Same-Source-IP-30，Same-Destination-IP-1，Same-Destination-IP-5，Same-Destination-IP-30 和 Same -Vulnerability-30 共 10 个属性。根据这 10 个属性从数据集 DATA1 中随机抽取 20%形成数据集 $D_{\mathrm{SVM\_Tr}}$，由数据集 DATA2 的全部数据形成 $D_{\mathrm{SVM\_Te}}$，分别作为支持向量机的训练和测试数据。本文使用交叉确认法

来训练数据，限于篇幅，只给效果最佳的一组结果。其中的参数错分样本的惩罚因子 $C=1.4$ ，RBF 核函数的控制因子 $g=1/\sigma^2$ 取 9，支持向量的个数为 1362 个，分类精度为 98.3556%。对照标定的结果，可得出：检测到的真报警有 2432 个，检测到的误报警有 13418，遗漏了 41 条真报警，真报警率为 98.3421%，误报减少率为 98.358%，漏报增加率为 1.6579%。测试时间为 3s，平均每条数据的测试时间约为 0.2ms(PⅣ 2.6GHz，内存 512MB)。

本文同时在相同的计算机上使用 19 个属性对 DARPA99 数据集进行 SVM 分类(记做 SVM-All)，与 RS-SVM 分类结果比较表明，在分类精度基本不变的前提下， RS-SVM 方法的支持向量减少了 357 个，总运行时间提高了近 5 倍。与文献中使用相同数据集和相同的 IDS 的结果比较(其余的文献由于使用了不同数据或者不同的 IDS 而不具备比较性)，结果表明了本文的方法具有一定的优越性，详细数据如表 1 所示。

表 1 RS-SVM 与相关文献的方法的结果比较

方法	TP	DFP	IFP
RS-SVM	98.3556%	98.358%	1.6579%
ALAC	99.46%	97.5%	2.4%
KNN	—	93%	0

5 结束语

本文从报警的根源性和时间性出发，总结出了区分真报警和误报警的19个相关的属性，并利用粗糙集理论对这些属性进行约简；将具有约简后10个属性的报警数据集上的过滤误报警的问题转化为数据分类问题，采用高效的支持向量机理论构造分类器。实验使用Snort监控DARPA99数据产生的报警数据，结果表明基于粗糙集-支持向量机理论的过滤误报警方法在漏报增加率为1.6579%的代价下，误报减少率可高达98.358%。下一步的工作就是在过滤了误报警的报警数据集上分析黑客的攻击目的，重现黑客的攻击场景。

参 考 文 献

[1] Julisch K. Using root cause analysis to handle intrusion detec-tion alarms. [PhD thesis], University of Dortmund, 2003.

[2] Manganaris S, Christensen M, and Zerkle D, *et al*.. A data mining analysis of RTID alarms. *Computer Networks*, 2000, 34(4): 571–577.

[3] Wang J and Lee I. Measuring false-positive by automated real-time correlated hacking behavior analysis. Information Security 4th International Conference, Košice, Slovakia, Heidelberg: Springer-Verlag, 2001: 512–535.

[4] Alharby A and Imai H. IDS false alarm reduction using continuous and discontinuous patterns. Proceeding of Applied Cryptography and Network Security. New York, USA, Heidelberg: Springer-Verlag, 2005: 192–205.

[5] Shin Moon Sun, Kim Eun Hee, and Ryu Keun Ho. False alarm classification model for network-based intrusion detection system. Proceeding of the 5th International Conference on Intelligent Data Engineering and Automated Learning, Exeter, UK, Heidelberg: Springer-Verlag, 2004: 259–265.

[6] Pietraszek T. Using adaptive alert classification to reduce positive in intrusion detection. Proceeding of the 7th Inter-national Symposium on Recent Advance in Intrusion Detection, Riviera, France, Heidelberg: Springer-Verlag, 2004: 102–124.

[7] Zhang Z and Shen H. Suppressing false alarms of intrusion detection using improved text categorization method. Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service, Taipei, Taiwan, Estats Units: IEEE Computer Society Press，2004: 163–166.

[8] Law Kwok Ho and Kwok Lam For. IDS false alarm filtering using KNN classifier. Proceeding of the 5th International Workshop on Information Security Applications, Jeju Island, Korea, Heidelberg: Springer-Verlag, 2004: 114–121.

[9] Walczak B and Massart D L. Rough sets theory. *Chemomet-rics and Intelligent Laboratory Systems*, 1999, 47(1): 1–19.

[10] Vapnik V N. An overview of statistical learning theory. *IEEE Trans. on Neural Networks*, 1999, 10(5): 988–999.

肖 云： 女，1978 年生，博士生，研究方向为网络安全与信息融合.

韩崇昭： 男，1943 年生，教授，博士生导师，研究方向为信息融合及其应用、复杂系统的建模与仿真等.

郑庆华： 男，1969 年生，教授，博士生导师，研究方向为网络安全、网格计算等.

赵 婷： 女，1982 年生，硕士生，研究方向为网络安全.