基于改进的粗糙神经网络模型的入侵检测系统研究

徐远纯　谭小萍
（景德镇陶瓷学院信息工程学院　景德镇 333001）

摘　要　本文对传统的粗糙神经网络模型进行了改进，加入了具有不良信息过滤功能的隐单元，在此基础上提出了相应的网络入侵检测模型，充分发挥了粗糙集理论和神经网络的优势，弥补了各自的缺点。实验证明，在传统神经网络里加入具有不良信息过滤功能的隐单元，可以有效识别网络中的不良信息，降低神经网络系统的输入维度，提高入侵检测系统的识别效果。

关键词　粗糙神经网络，入侵检测，不良信息过滤，模型

Research of Intrusion Detection System Based on Improved Rough Neural Network

XU Yuan-Chun　TAN Xiao-Ping
(College of Information Engineering, Jingdezheng Ceramic Institute, Jingdezheng 333001)

Abstract　In this paper, the traditional rough neural network model is improved, adding a hiding unit with function of filtrating harms information. Then an intrusion detection model is proposed to show the advantages of both rough sets and neural network. With running an example, this model can identify harm information in WebPages and improve the efficiency of intrusion detection system obviously.

Keywords　Rough neural network, Intrusion detection, Filtrating harm information, Model

神经网络(NN)作为人工智能领域的一个重要分支，具有强大的数值逼近能力，它能够处理定量的、数值化的信息，在很多领域已经得到了颇为广泛的应用。但作为神经网络的输入必须是一些量化的数值型数据，这在某种程度上限制了它的应用范围。粗糙集(Rough Sets，RS)理论是一种刻画不完整性和不确定性的数学工具，能有效地分析和处理不精确、不一致、不完整等各种不完备信息，并从中发现隐含的知识，揭示潜在的规律。在RS理论中，对象用其属性集合表示，分类用来产生概念，概念构成知识的模块，知识是由对象论域的分类模块组成的，它提供关于现实的明显事实，同时也具有由明显事实推导出模糊事实的推理能力。粗糙集理论的出现在某种程度上可以弥补神经网络对数据结构比较敏感的弱点，提高神经网络的泛化能力，于是就产生了所谓的粗糙神经网络系统。粗糙神经网络系统就是将粗糙集与神经网络结合，利用RS来简化NN的训练样本，在保留重要信息的前提下消除冗余的数据，从而提高训练速度和训练效果。

1　粗糙神经网络系统的研究现状

粗糙集约简可以化简神经网络的训练数据集，在保留重要信息的前提下消除多余的数据，减少数据输入的维数和神经网络的计算量。目前，有两种利用粗糙约简简化神经网络的方法。

(1)利用粗糙约简简化神经网络输入维数

神经网络的结构受输入网络的数据的维数影响很大，同时，数据的维数也影响到决策规则的数目、网络的计算量，甚至影响到神经网络的收敛。因此，适当地利用粗糙约简降低作为输入神经网络系统的数据维数可以更好地实现网络系统。

(2)利用粗糙约简简化模糊神经网络规则数

模糊神经网络是基于模糊推理的原理形成的系统，系统的结构受模糊规则的个数影响较大。在实际应用中，规则数过多会导致系统不能收敛和网络的训练时间长或训练误差大等等缺点，因此，利用粗糙约简模糊神经网络的决策规则数，可以大大减小网络的计算量，加快网络的收敛速度。

一个典型的粗糙神经网络系统通常由四层组成，经过各层的运算可以实现不可分辨关系的划分和利用神经网络进行推理，即构造了具有粗糙推理功能的系统。

第一层为输入层，这与普通神经网络系统相同，接收系统的数据输入 $X=(x_1,x_2,\cdots,x_n)^T$。网络对输入层的权值都设为1，且在训练中不作任何调整，即

$Netoutput=O_i=Netinput=(x_1,x_2,\cdots,x_n)$

第二层是粗糙隶属度计算层，根据粗糙集理论对输入向量不可分辨关系按照粗糙隶属度进行划分，将每个输入分量离散化为 k 个不可分辨关系的隶属度，一般采用高斯函数作为粗糙隶属度的计算函数，即

$$\phi_i(x^p)=\exp\left(-\frac{(\|x_p-c_i\|)^2}{\sigma_i^2}\right)$$

第三层：推理层，该层的每个节点代表一条规则，这些规则是通过粗集理论得到的。若有 m 条规则，则输出 $O_{3i}=\mu_{1i}\mu_{2i},\cdots,\mu_{ni},1\leqslant i\leqslant m$。其中 $\mu_{ij}=O_{ij}^2$。

第四层：输出层，在该层实现了多输入单输出系统，输入为第三层的输出 O_{3i}，其中权值 w_i 预先设定，网络训练时可调整。输出为 $Output=\sum_{i=1}^{m}w_iO_{3i}$。

目前粗糙神经网络系统已经在某些领域得到初步的应用，但在涉及到计算机安全的入侵检测领域尚没有较好的解决方案。本文针对计算机网络安全问题的特点，对常用的四层粗糙神经网络模型进行了改进，增加了一层具有信息过滤

徐远纯　副教授，硕士，主要研究方向为计算机网络；谭小萍　讲师，主要研究方向为高教管理和计算机技术。

功能的隐单元，使整个粗糙神经网络系统具有 Web 信息过滤的功能，从而提高了入侵检测系统的实际应用效果。

2 改进后的基于粗糙集理论的神经网络模型

越来越多的计算机实践证明，很多计算机网络系统遭到病毒入侵、木马控制等都是由于打开了含有不良信息的网页造成的，因为这些木马程序和代码很多都藏身于不良网页中，如以色情、赌博、反动等为主题的网站。基于此，本文在神经网络系统中构造了一个具有不良信息过滤功能的隐单元，对网页信息进行先期过滤，以便最大程度地发挥神经网络系统检测入侵行为的作用。

我们通过前期研究工作发现，大量的不良网页除网页文本正文、图片之外，在网页框架格式、各种暗示性条文、页面超链接元素等方面较一般网页都有其显著的特点，而以上这些网页结构化特征在一般文本过滤或分类系统中常常在预处理阶段就被去除掉了，一定程度上影响了信息过滤的实际效果。因此，本文所构造的具有不良信息过滤功能的隐单元拟从最关键的文档内容方面提取不良网页的特征。目前互联网上的网页主要以 HTML 形式存在，HTML 语言通过使用描述性的标记符(标签)来指明文档的不同内容。标签是区分文本各个组成部分的分界符，用来把 HTML 文档划分成不同的逻辑部分，如段落、标题和表格等。标签描述了文档的结构，它向浏览器提供文档的格式化信息，以传送文档的外观特征。

针对 Web 文档内容的特征提取，我们首先抽取 Web 文档的核心文本，对文本进行分词，去除停用词、合并同义词、近义词、进行词频统计；提取文本特征项。我们采用常用的 TF-IDF 公式计算词条权值：

$$\Phi_k(d)=\frac{tf_{ik}(d)\log(\frac{N}{n_k}+0.01)}{\sqrt{\sum_{k=1}^{n}tf_{ik}^2(d)\times\log^2(\frac{N}{n_k}+0.01)}}$$

其中，$f_{ik}(d)$表示词条 t_k 在文档 d 中出现的频率，N 表示全部样本文档的总数，n_k 表示包含词条 t_k 的文档数。此外还需考虑词条的位置信息，例如文章标题、副标题、关键字中的词条要全部保留下来作为特征项，并赋予较高的权重。

Web 信息过滤的工作可以被看作是一个分类的问题。Web 页面被视为一个文档文件，是否需要过滤可以看成一个分类标签(即决策属性 D)，在此我们分别将其编码为 1 和 0。以 Web 中提取的特征项作为条件属性集，文本是否需要过滤作为决策属性集建立决策表。其中条件属性集中包含了网页的布局、PICS(因特网内容选择平台)等级评定应用，暗示性条文和文档内容四个方面的特征。

具有不良信息过滤功能的隐单元所要实现的功能就是对每一个 HTML 网页中的有嫌疑信息从上述四个方面进行比对，利用 TF-IDF 公式计算 $\Phi_k(d)$值，并与预先设定的阈值进行比较，如果超出阈值范围，说明该信息有较大的可能属于不良信息，在进行下一步之前加以过滤，如果在安全范围内，则顺利通过，继续检测其它的 HTML 网页。阈值的确定是在文本的训练阶段，从训练文本中提取的具有较高维数的信息，利用 TF-IDF 公式从所有出现过的单词中提取权值较高的词条作为特征词构成条件属性集。特征词按权值大小进行降序排列，形成阈值数据集。

显然，改进后的基于粗糙集的神经网络对于多输入单输出的情况而言，输入向量的各分量在决策中起决定性作用的是该分量的网络权值 w_i。若权值 w_i 较小或者为零，即该输入 x_i 在系统中是不重要的或不起作用的。另外，如果输入向量 $x_{ij}\neq1, j=1,2,\cdots,n$ 的权值 w_j 较大，而 x_i 权值 w_i 相对较小，则该输入 x_i 在系统中是不重要的。因此，可以删除这些在网络中不起作用的输入。对于多输入多输出的情况，则要复杂一些，因为每个输入 x_i 都有 n 个权值 w_{ij}。不过，当某个输入 x_i 的权值 $w_{ij}=1,2,\cdots,n$ 比其它输入的都较小时，可以适当地调整权值 $w_{ij}=1,2,\cdots n$，使 w_{ij} 更接近于零，如果网络仍然稳定和保持正确分类，则可以先约去输入向量中第 i 个输入分量，重新将 $n+1$ 个分量作为网络的输入，同时删除第 i 个输入结点，其它结点仍用原网络的权值。可能这种约简会产生一些误差，可以适当地调整网络的权值，如果出现网络不稳定和错误，说明这个条件属性是重要的。如此循环进行，直到不可约简为止。

3 基于改进后粗糙神经网络的入侵检测系统模型

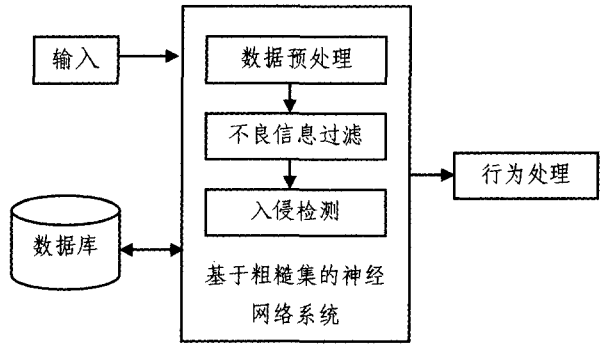

图 1 基于粗糙神经网络的入侵检测系统

基于粗糙神经网络的入侵检测系统如图 1 所示，主要包括输入、用基于粗糙集的神经网络系统进行检测、行为处理三部分。该粗糙神经网络模型具有学习速度快、隐层节点少、容错能力强等特点。

(1)输入模块在实际应用中负责抓取网络中的数据包，对数据进行初步提炼后送至神经网络系统进行处理。其主要功能是捕获和过滤流向监控主机的网络数据包。数据包捕获功能用来在网络上截获并阅读位于 OSI 协议模型(TCP/IP)中各个协议层上的数据包。数据包捕获的基本原理是利用 Socket 编程设置网卡为混杂模式，在该模式下可以截获所有的数据包，而不管其物理地址如何。数据包过滤功能用来过滤掉那些目的 IP 地址不是本地主机的数据包，并对捕获的数据包进行解析，过滤掉除 IP，TCP，UDP 和 ICMP 协议之外的数据包。之后，将捕获的 IP，TCP，UDP 或 ICMP 的数据包进行解析，并把解析结果发向预处理模块。

(2)接收到输入数据之后，就进入神经网络系统进行处理，一般要经过三个步骤，即数据预处理、不良信息过滤和入侵检测。预处理模块负责将数据采集模块送来的原始数据进一步加工处理。对捕获的数据包进行检测前，还要进行协议分析。使用高层协议分析技术，加入对应用层协议的解码和状态分析。根据数据包中的协议信息逐层分析，依次解析出各层次协议，直至应用层。然后按照所属协议的类型，详细分析潜在的攻击行为。这样做虽然加大了检测的复杂性，但减小了匹配区间，可以极大地提高检测的准确性，并能检测到某些协议异常的未知攻击，可以降低误报率。

(3)行为处理模块就是根据系统的检测判断结果进行相应的处理，对检测到的异常行为，根据用户定义的响应策略进行报警或采取相应的措施。数据库保存入侵检测系统收集到的所有事件信息，包括正常和异常事件，以利于提高整个系统的识别效果。

4 实例应用

本文使用UCI数据库提供的网络入侵测试数据集进行实验分析。该数据集中包括正常数据和两种异常数据，每种数据包括网络数据包的包头信息、网络连接和传输信息等37个属性，将数据集分为训练集和测试集两部分。

(1)首先对原始数据进行预处理，将原始数据中的噪声去掉并转换为神经网络可处理的特征向量。原始数据属性包括：UKEY，ID，diff_source_hosts，dst_bytes，duration，serror_rate，SYN等37个属性，限于篇幅，此处不一一列出。使用粗糙集方法将原始数据中多余的和不相关的信息去掉，删除与本文采用的入侵检测方法无关的属性。

(2)将神经网络无法处理的符号字段转换成数值字段。将部分属性重新编码，如将ACK，PSH，FIN，SYN，URG属性中的值"NULL"用"0"替换。destination_host和source_host属性表示IP地址，分别为其增加一个新的属性，表示IP地址中前两段的网络号信息，内部网络IP地址用"0"值，外部网络IP地址用"1"值。

(3)对各属性值进行归一化处理，减少由于记录间字段数值差异过大而对网络训练产生的不良影响。将dst_bytes，duration，destination_port，source_port属性的值除以10得到0～6.5535之间的数值。

(4)将经过数据预处理的条件属性用改进后的神经网络系统进行训练，并在测试集中进行入侵检测试验。为检验模型的泛化性能，我们将训练集分为两组，第一组在训练集中选取40条记录作为训练样本数据，每一类数据各20条；第二组在训练集中选取100条记录作为训练样本数据，每一类各50条。测试时，在测试集中各选取50条正常数据、50条问题数据。限于篇幅，训练及测试过程略。

(5)将结果与训练集进行比对。鉴于有效降低入侵检测的误报率及漏报率是入侵检测的公认难题，我们用误报率作为标准进行比较。两种算法在两组不同数据集的检测结果(误报率)如表1所示。

表1 两种系统进行入侵检测的误报率

误报率(%)	传统神经网络系统	改进后的神经网络系统
第一组	23.6	19.1
第二组	36.2	25.5

由此可以看出，使用相同训练样本训练而得到的网络模型进行测试，改进后的系统入侵检测识别能力明显好于传统粗糙神经网络。尤其是经过不良信息过滤隐单元的过滤，在入侵检测前期就去掉了大量的明显的网络入侵信息，简化了神经网络的输入维度，从而使整个入侵检测系统的误报率显著降低。

结束语 互联网中的入侵、黑客行为非常繁杂，有的显而易见，有的则需要专门的入侵检测系统进行专门检测。本文对传统的基于粗糙集的神经网络系统进行了改进，将Web信息过滤技术加入入侵检测系统，先期过滤掉能够明显识别的入侵信息，以减轻神经网络系统的运行负荷，提高了入侵检测系统的适用性。

参考文献

1 唐正军. 网络入侵检测系统的设计与实现. 北京：电子工业出版社，2002

2 Lippmann R P, Cunningham R K. Improving Intrusion Detection Performance Using Keyword Selection and Neural Networks. Computer Networks—the International Journal of Computer and Telecommunications Networking, 2000, 34 (4) : 597～603

3 蒋建春，马恒太，任党恩，等. 网络安全入侵检测：研究综述. 软件学报，2000(11)：1460～1466

4 单征. 基于网络状态的入侵检测模型. 信息工程大学学报，2002(3)：9～14

5 周志华，曹存根. 神经网络及其应用. 北京：清华大学出版社，2004

(上接第62页)

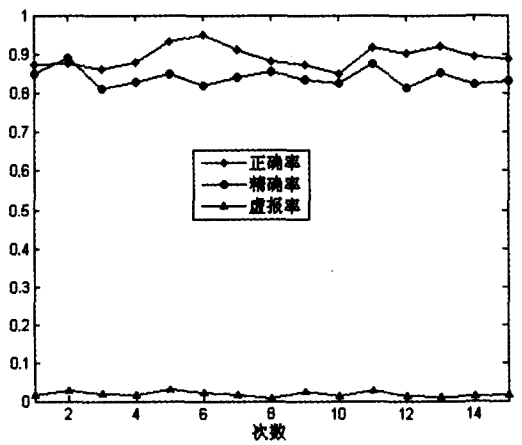

图4 过滤性能指标曲线图

从图4可以看出，正确率和精确率都比较稳定，说明系统的识别能力良好，虚报率较低且值的变化较小，说明系统将正常邮件识别为垃圾邮件的概率较低，即使在这种情况下，由于具有协同刺激机制，邮件也不会被误删，说明系统具有较高的可靠性。此外，影响结果的因素有很多，例如成熟细胞的激活阈值、可信任邮件数目等，部分参数是相互作用的，应保持合适的比例。

小结 本文提出了一种基于免疫机制的智能反垃圾邮件过滤器，主要完成邮件分类、抗体库更新和对用户反馈的协同认证等。该过滤器可以识别垃圾邮件的特征变化并学习、记忆新的垃圾邮件特征，从新的垃圾邮件内提取特征向量，学习用户的行为习惯。系统首先使用可信任邮件列表和黑地址列表对邮件进行初次筛选，其余邮件则由基于免疫的过滤器进一步审查，这种双层机制减少了对一些特征明显的邮件的审核，在提高判别效率的同时进一步增强了系统的可靠性。性能测试表明，IISF对垃圾邮件具有良好的识别能力，并具备一定的自学习和自适应性。

参考文献

1 李涛. 基于免疫的网络监控模型[J]. 计算机学报，2006，29(9)：1515～1522

2 肖人彬，王磊. 人工免疫系统：原理、模型、分析及展望. 计算机学报[J]，2002，25(12)：1281～1293

3 Dasgupta D, Attoh-Okine N. Immunity-based systems: A survey. In: Proc. IEEE International Conference on systems[C], Man and Cybernetics, 1997. 369～374

4 李洋，方滨兴，王申. 基于用户反馈的反垃圾邮件技术[J]. 计算机工程，2007，33(8)：130～132

5 Perone M. An Overview of Spam Blocking Techniques[R]. Barracuda Networks Corp, 2004

6 张修文，吴伟志. 粗糙集理论与方法[M]. 北京：科学出版社，2001. 12～39