苏州大学学位论文使用授权声明

本人完全了解苏州大学关于收集、保存和使用学位论文的规定，即：学位论文著作权归属苏州大学。本学位论文电子文档的内容和纸质论文的内容相一致。苏州大学有权向国家图书馆、中国社科院文献信息情报中心、中国科学技术信息研究所（含万方数据电子出版社）、中国学术期刊（光盘版）电子杂志社送交本学位论文的复印件和电子文档，允许论文被查阅和借阅，可以采用影印、缩印或其他复制手段保存和汇编学位论文，可以将学位论文的全部或部分内容编入有关数据库进行检索。

涉密论文□

本学位论文属　　在_____年___月解密后适用本规定。

非涉密论文☑

论文作者签名：陈熹　　日　期：2012.4.15

导师签名：　　日　期：2012.4.15

基于神经网络的入侵检测系统的研究与设计

摘要

现今计算机网络安全问题已越来越受人们关注，网络入侵的手段越来越复杂多样化。由于传统的网络安全防护技术的具有局限性，使入侵检测系统成为了目前网络安全技术的研究热点。针对现有入侵检测系统的一些缺点，本文将人工神经网络应用于入侵检测系统中，取得了较明显效果。

论文首先阐述了入侵检测技术的特点，入侵检测系统(IDS)的基本模型，研究了Kohonen 神经网络和 BP 神经网络的学习方式和数学推导。

接着，依照模块化的思想设计了一个基于神经网络的入侵检测系统，并对模块分别进行详细的设计。考虑到网络数据流的庞大，在系统中加入了特征提取模块，该模块运用了主成分分析技术，通过对数据进行空间变换消除冗余降低数据维数，提高系统实时响应能力。针对 BP 算法存在的一些缺陷，介绍了 6 种改进方法。

最后，在 Matlab 平台上进行实验仿真得出实验结果并进行对比分析。对 KDD99 数据集用 Python 语言进行数据预处理，并从中提取出四种攻击类型的训练样本和测试样本，分别将未经主成分分析特征提取技术和经过该技术的数据送入 Kohonen 神经网络和 BP 神经网络进行训练和检测。将检测率、误报率、训练时间和检测时间作为入侵检测系统的性能评价标准。在对 Kohonen 网络的实验中发现主成分分析特征提取技术缩短训练和检测时间的效果有限，对攻击的检测率较低，误报率较高，无法满足入侵检测系统的基本要求；在 BP 神经网络的实验中，通过比较得出检测四种攻击类型的最佳算法，PCA 特征提取技术和改进的 BP 算法两者均可以减小网络训练未收敛的几率，缩短训练时间和检测时间。对比 Kohonen 网络和 BP 网络的实验结果：数据通过主成分分析特征提取后经过改进 BP 神经网络进行入侵检测的检测率很高、误报率较低、实时响应快，是一个高效可行的技术方法。

关键字：网络安全；入侵检测系统； BP 神经网络；Kohonen 神经网络；特征提取

作　　者：陈　熹

指导教师：朱灿焰

Research and Designation of Intrusion Detection System Based on Neural Network

Abstract

Nowdays, the computer network security issues have been more and more concerned. The means of network intrusion become increasingly complex and diversified. Due to the limitations of traditional network security technologies, intrusion detection systems turn into the focus research of the network security technologies at present. To improve some shortcomings of the existing intrusion detection systems, this thesis applied artificial neural networks to the intrusion detection systems (IDS), and it comes up with good results.

In the paper, the characteristics of intrusion detection technologies, the basic model of IDS, are first described; the learning principle and mathematical derivation of the Kohonen and BP neural network are studied.

Then an intrusion detection systems based on neural network is designed in accordance with the idea of modular, and each module is devised in detail. Taking into account the large network datastream, a feature extraction module is added into the system. The principal component analysis technology is applied in this module. It can eliminate redundancy and reduces the dimension by means of data space transformation, so it can improve the ability of the system real-time response. Also to solve weak points of BP algorithm, six kinds of improvements are introduced in this paper.

Finally, experiment simulation results are obtained by Matlab platform. First, preprocess the KDD99 data sets with Python language; Extracted the training samples and testing samples of the four types of attacks from KDD99 data sets, BP and Kohonen neural network is implemented to train and test the extracted data, whether the data is processed by PCA feature extraction procedure or not. Then compare and analyze the results by using Detection rate, false alarm rate, training time and testing time as the performance evaluation criteria. It is concluded those by the results, as in the experiments of the Kohonen network, principal component analysis is limited to shorten the training and testing time; in the BP neural network experiments, get the best algorithms to detect four types of attacks by comparison, the PCA feature extraction technology and improved BP

algorithm can both reduce the chance of convergence of network training, reduce training time and testing time. Compared with the experimental results of the Kohonen network and BP network, we also conclude that the data which is processed by PCA feature extraction procedure have a high true positive rate, a low false positive rate and a quick real-time response when detected by BP neural network, and this method is an efficient and feasible technique.

Keywords: Network Security; Intrusion Detection System (IDS); BP Neural Network; Kohonen Neural Network; Feature Extraction.

Written by: Xi Chen
Supervised by: Canyan Zhu

目 录

第1章 绪论

1.1 课题背景及意义

随着互联网技术在经济、科研、军事及人们日常生活中的普及，人类越来越离不开互联网。网络购物、团购、社交网站、网络游戏和微博等互联网业务发展迅速，丰富了人们的生活，带来许多便利。截至2011年12月底，我国网民规模达到5.13亿[1]，互联网普及率达到38.3%，全年新增网民5580万人，网络购物使用率提升至37.8%，去年新增用户3344万人，团购应用发展势头迅猛，用户已达到6465万人，使用率提升至12.6%，较2010年底上升8.5个百分点。团购用户年增长率高达244.8%，成为全年增速第二快的网络服务。

在网络快速发展的同时，计算机网络安全问题也越来越受人们关注。2011年上半年，我国约有2.17亿网民遭到病毒或木马攻击[1]，占整个网民的44.7%，有约1.21亿人有账号或密码被盗的经历，占24.9%. 近年来，有约3880万网民在近半年碰到过网上欺诈行为。网络安全事件大幅度增加，网络和信息安全面临着严峻的形式。

2010年1月12日，全球最大的中文搜索引擎百度的DNS服务器遭黑客劫持，5个多小时无法访问，百度CEO李彦宏惊呼这次事件是“史无前例的”。2011年4月，索尼PlayStation网络遭遇入侵，被黑客攻击10余次，导致1亿多个用户账户曝光。同年6月，美国花旗银行系统被黑客入侵，21万北美地区银行卡用户的姓名、账户、电子邮箱等信息被泄露。12月，发生了堪称中国互联网史上最大的泄密事件—“CSDN泄密事件”，CSDN的安全系统遭到黑客攻击，600万用户的登录名、密码及邮箱遭到泄漏，随后，CSDN"密码外泄门"持续发酵，天涯、人人网、开心网、世纪佳缘等知名网站相继被曝用户数据遭泄密，网上公开暴露的网络账户密码超过1亿个。随着第三代移动通信(3G)的来到，笔记本电脑、无线路由器和DA等无线接入设备，也开始成为攻击的新目标。

中国互联网络安全中心发布的近几年中国电脑病毒疫情的报告表明，病毒的入侵攻击变得越来越频繁。犯罪份子为了获得金钱制作了越来越多的黑客软件。黑客入侵的手法趋于多元化：网上木马、间谍程序、钓鱼网站、僵尸网络等等。这些计算机犯

罪已经成为影响网络发展、特别是商业应用的主要问题，造成了巨大的经济损失，直接威胁着国家和社会的安全。

目前面临的网络安全威胁主要有这几个因素：黑客的攻击、软件漏洞、网络协议的缺陷等[2]。网络安全问题未能引起一些企业的重视也是一个因素。传统的网络信息安全的防护技术如防火墙有着自己的局限性。首先，防火墙[3]在错误的系统配置或安全策略下不能抵御某些入侵，并且对来自内部的攻击毫无办法。其次，防火墙是一种被动的保护，入侵者可以绕过防火墙实现入侵。单靠防火墙是不能满足现今网络安全的需要，必须设立多道安全防线，综合各种网络安全防御机制。

解决上述问题的方法是建立一个入侵检测系统。入侵检测系统[4]具有主动防御的特点，它能够捕获并记录网络上的动态数据信息，分析出可能出现的异常情况，识别入侵者和入侵行为，并进行实时响应或防护，包括切断网络连接和报警等。因此，研究入侵检测有着非常重要的意义。

1.2 国内外研究现状

入侵检测的研究开始于上世纪 80 年代，1980 年当时负责主持美国国防部计算机安全审计工作的詹姆斯·安德森首次提出了入侵尝试[5](Intrusion attempt)或威胁(threat)的概念。

1986 年，斯坦福研究院(SRI)的多罗西·丹宁发表了一篇论文《An Intrusion Detection Model》[6]，首次建立了一个完整的入侵检测系统(IDS)模型，这篇文章后来被认为是入侵检测系统的开山之作。

1990 年，美国加州大学戴维斯分校设计出了第一个基于局域网的入侵检测系统，第一次将网络数据包作为审计数据源。

1994 年，美国空军密码支持中心建立了一个入侵检测系统 ASIM，该系统主要应用于美国空军，并开始向商业推广。

1997 年，思科公司收购了 Wheelgroup 公司，并在其路由产品中加入 IDS,掀起了将入侵检测技应用于网络的革命。

随着 Internet 的发展和普及，许多类型的入侵检测系统应运而生，目前的入侵检测系统大致可以分为两类[7]：基于主机的 IDS 和基于网络的 IDS。

从入侵检测的研究产品来看，国外的产品处于领先地位，我国由于起步比较晚，基础比较薄弱，成熟的产品不多，多是停留在理论研究阶段。斯坦福大学、加州大学戴维斯分校、麻省理工学院在网络安全领域有着先进的研究水平。国外相关的主流产品有[8]：Cisco 公司的 NetRanger 系列 、Internet Security System 公司的 RealSecure 、Intrusion Detection 公司的 Kane Security Monitor 、Axent Technologies 公司的 OmniGuard/Intruder Alert 、Trusted Information System 公司的 Stalkers 等。国内的一些高校如中科院、清华大学、北京邮电大学、哈尔滨工业大学的科学研究实力处于前列。在产品方面主要有[9]：中科网威的“天眼”入侵检测系统 、启明星辰的 SkyBell(天阗) 、绿盟科技的 NSFOCUS NIDS 系列等。近几年国家对互联网和信息安全越来越重视，加大了这方面的投入，各高校科研经费逐年增加，理论研究和技术上与国外的差距正在不断缩小。

1.3 研究的主要工作和内容安排

1.3.1 主要工作

本文的主要工作有以下几个方面：

(1)介绍了入侵检测的基本概念，讨论了常用的入侵检测技术的特点，分析了入侵检测系统的常用模型。

(2)研究了 BP 和 Kohonen 神经网络，将神经网络应用于入侵检测系统中，完成了一个基于神经网络的入侵检测系统的研设计。引入 PCA 特征提取技术来减小神经网络算法的运算量，对 BP 神经网络算法进行改进以提高检测效果。

(3)利用 KDD99 数据集对两种不同神经网络算法的入侵检测系统进行实验验仿真和结果分析，得出四种攻击类型的最优算法，并通过对比分析了 PCA 特征提取技术、两种神经网络算法的优缺点。

1.3.2 论文内容安排

全文共分为六章：

第一章为绪论，主要介绍了入侵检测系统的研究及意义，国内外的研究现状和本文的主要研究内容和章节安排。

第二章是主要阐述了入侵检测的概念，入侵检测系统的评价标准和主要结构，入侵检测系统的标准模型以及入侵检测技术的未来发展趋势。

第三章研究了人工神经网络的主要特点，Kohonen 神经网络和 BP 神经网络的基本原理和算法的数学推导，分析了神经网络在入侵检测系统的中的优势。

第四章设计了一个入侵检测系统的结构，对结构的各模块进行详细说明，在结构中应用了主成分分析的特征提取技术降低数据维数，针对传统 BP 算法的不足进行改进。对 KDD99 数据集进行数据预处理工作，并对入侵检测系统中的 Kohonen 网络和 BP 网络进行了具体的网络参数设计。

第五章对第四章设计的入侵检测系统进行实验仿真。将 PCA 特征提取技术和 Kohonen 网络和 BP 神经网络相结合，对各种算法的实验结果进行比较和分析，得出结论。

第六章是对工作的总结及展望。

第2章 入侵检测系统及相关技术

2.1 入侵检测技术概述

2.1.1 入侵检测介绍

入侵[10]，是指在没有获得许可的情况下，对计算机系统或信息系统进行操作，危及系统保密性、可靠性的行为。入侵分为两种情况[11]：外部入侵和内部入侵。外部入侵指来自系统外的威胁，如黑客入侵、自然灾害；内部入侵指出自系统内部的威胁，一般是合法用户的误操作或越权行为。入侵可以使系统无法正常工作，导致数据丢失，信息窃取，有的可能造成系统无法提供服务。入侵检测就是察觉上述入侵行为的过程。入侵检测的手段包括监控计算机网络系统的状态、行为和运行情况，分析处理网络关键节点的信息，审计数据，检测系统用户的超越使用权限的非法行为以及外部入侵者的入侵行为。入侵检测具有实时监控、动态响应、易于配置的特点。因为入侵检测能帮助系统检测和阻止网络入侵，并且增加了网络管理员的安全审计、监视、攻击识别和响应等能力，提高了系统的安全性，所以被认为是防火墙的有效补充。入侵检测技术的出现，给系统管理带来了主动性，进一步提高了网络的可靠性和安全性。

目前，解决网络安全问题的主要技术手段[12]有数据加/解密技术、数据鉴别技术、防火墙技术、访问控制技术等，这些传统的网络安全技术主要采取的是被动的防御手段，通过检测入侵或日志等来发现网络、系统中的攻击行为，其特点是在遭受攻击后，只能茫然等待下一次攻击的到来，不能主动对攻击行为进行控制和反击。因此，各种防御技术都有其局限性。要想更好的保证网络的安全，单靠一种防御技术是无法达到要求的，只有综合运用多种防御机制，建立多道安全防线（例如将防火墙、加密技术和身份认证技术与入侵检测技术结合起来），完善安全防御体系，才能有效的抵御来自系统内外的入侵。

2.1.2 入侵检测系统的评估指标

入侵检测系统在设计完成之后，需要进行测试评估，看其是否到达设计目标。目前来说对于入侵检测的常用评估指标有[13]检测率、误报率、漏报率等。

检测率是指被监控系统受到入侵攻击时，入侵系统能够检测到的概率，可表示为：被发现的攻击样本数/攻击样本的总数。

误报率是指把正常的行为判断为入侵行为而进行报警的概率，可表示为：被误判的正确样本数/正确样本的总数。

漏报率是指被监控系统发生入侵行为时，检测系统没有检测出入侵行为的概率，可表示为：被误判的正确样本数/攻击样本的总数。

目前在国际上也用接受机特性[14]（Receiver Operating Characteristic，ROC）曲线来评价入侵检测系统的性能，如图 2-1。

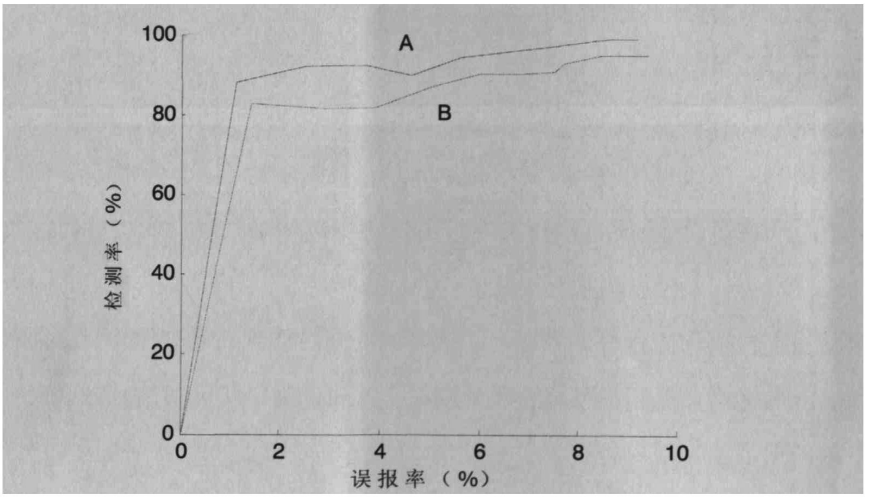


图 2-1 ROC 曲线例图

ROC 曲线用图形的方式来表示正确率和误报率之间的关系，曲线越靠近坐标的左上方，曲线的下方区域越大，说明入侵检测系统的准确率越高。用 ROC 曲线来评价入侵检测系统显得非常直观和有效。

此外，还有一些其它的性能评价指标，如抗攻击能力、检测延迟时间、系统负荷能力、检测范围等。

2.2 入侵检测系统

2.2.1 入侵检测系统的结构

入侵检测系统[15]是一种能够通过系统进行实时监控，分析网络的相关数据，检测到有可疑的入侵行为后进行警报等一系列措施的系统。一般的入侵检测系统的结构[16]

如图 2-2 所示，由信息提取、数据分析和响应处理三部分组成。

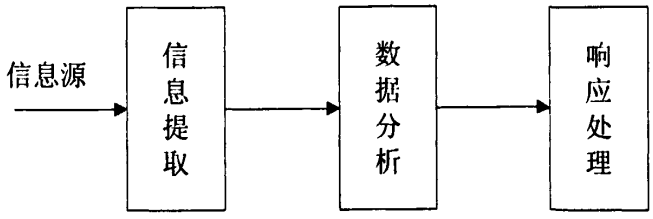


图 2-2 入侵检测系统的一般结构

1.信息提取

信息提取是入侵检测的第一步，含信息收集和数据预处理两个步骤。入侵检测系统需要在计算机网络系统的若干不同关键点（如不同网段和不同主机）收集信息。信息收集是从入侵检测系统的信息源中收集信息，它的内容包括系统、网络、数据以及用户活动的状态和行为。收集到的信息越多越可靠准确，入侵检测的检测效果就越好。收集到信息之后，就要进行数据预处理。因为原始收集的数据的质量将直接影响数据分析和用户特征的提取，所以需要通过预处理。信息的收集一般通过三个方面来获得：系统和网络日志文件、非正常的目录和文件改变以及非正常的程序执行。

2.数据分析

经过信息提取得出来的数据依然是海量，在这些数据中，正常信息（非入侵信息）占绝大多数，而入侵行为的信息只有一小部分，因此需要利用数据分析手段从庞大的信息量中找出异常信息。数据分析技术有很多种，常见的有完整性分析、模式匹配和统计分析等，每种方法各有优劣，并且各自应用的方向也有区别。

3.响应处理

当入侵检测系统检测到有入侵攻击时，就会依据预先定义好的响应机制采取措施。响应处理分两步进行，第一步是将检测结果和采取的措施写入日志文件，供网络管理员查看和以后的日志审查，记录的内容一般包括日期、时间、源地址和目的地址、描述与事件相关的原始数据，以及向系统管理人员发送报警的电子邮件等。第二步是系统对攻击做出的响应，要求迅速执行，如报警、用防火墙切断攻击源地址与系统的连接、过滤攻击者的 IP 地址、执行用户自定义的操作等。

2.2.2 入侵检测系统的分类

根据不同的分类标准，入侵检测系统可以分为不同的类别[17]：按照数据源的不同，

可以分为基于主机的 IDS 和基于网络的 IDS；按照所采用的分析技术来分类，可以分为异常检测 IDS 和误用检测 IDS；依照体系结构的差异，分为集中式、等级式、协作式 IDS；依照响应方式来分，可分为主动响应 IDS 和被动响应 IDS。根据反映时间的快慢，分为实时处理 IDS 和事后处理 IDS。下面介绍最常见的分类：基于主机的 IDS 和基于网络的 IDS。

1.基于主机的入侵检测系统(Host-based Intrusion Detection System,HIDS)

基于主机的入侵检测系统[18]是早期的入侵检测系统结构，重点检测主机系统和系统本地用户。它的数据源主要来自系统日志（如 Linux 的 Loginlog、Wtmp 和 history 文件），应用程序日志(如 Syslog 文件)，提取数据之后进行审计和数据分析，发现异常入侵行为并作出响应。基于主机的 IDS 还能对系统的重要文件进行实时监控，监听对主机的各服务端口，监视试图入侵系统的一切可疑行为。HIDS 的系统结构如图 2-3 所示。.

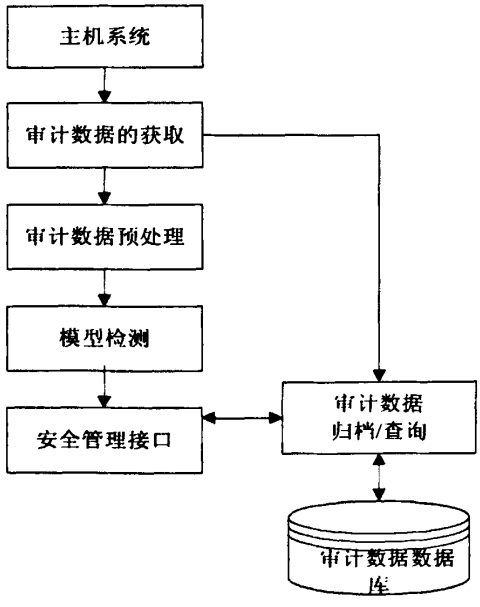


图 2-3 基于主机的入侵检测系统体系结构图

基于主机的入侵检测系统的基本原理是通过分析计算机操作系统的日志文件、应用程序的日志、系统调用和端口调用，比较这些审计数据文件的记录与攻击模式是否匹配，如果匹配，则检测系统向管理员发出报警并作出相应的行动。攻击模式是预先设置好的，在匹配规则库中用一种特定的方式来表示。HIDS 一般安装在重要的主机系统上，也可以部署在系统关键的路由节点。为了降低检测的误报率和漏报率，可以

将 HIDS 布置在网络的不同节点，设置管理节点和分节点。

基于主机的入侵检测系统的主要优点是：能够确定攻击是否成功；监控精确全面；适用于加密和交换环境；检测和响应迅速。

但另一方面，基于主机的入侵检测系统也有缺点：部署代价大；主机日志提供的信息有限；占用大量主机资源。

2.基于网络的入侵检测系统(Network-based Intrusion Detection System,NIDS)

NIDS[19]分析的数据是网络上的数据包，它通过网络适配器捕获和过滤网络数据包，随之进行入侵的识别和响应。其系统结构如图 2-4 所示。

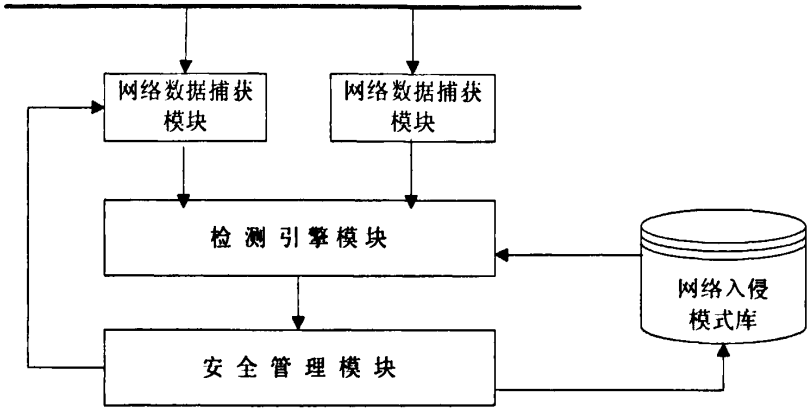


图 2-4 基于网络的入侵检测系统体系结构图

网络数据包捕获模块是网络入侵检测系统的基础。HIDS 将自己的网卡设置为混杂模式，就可以捕获整个网段内的网络数据包。常用的捕获数据包的工具有 ethereal 、sniffer 和 wireshark 等。网络数据包被捕获以后，需要包过滤机制进行过滤，以获得满足条件的数据包。

网络数据包经过过滤后，需要检测引擎模块对数据包进行处理和分析，从而发现数据流中的入侵事件和行为。所以检测引擎模块是 HIDS 的重要组成部分，它的好坏会直接影响 HIDS 的检测效果。

网络入侵数据库用来预先记录一些常用的攻击模式，这些模式用特定的形式表示。当检测引擎模块需要进行数据分析和检测时，就会查询该模式库进行特征匹配。

安全管理模块用来接收检测引擎模块的响应报告，并作出相应的响应。

NIDS 的优点[20]是成本较低，不需要安装在每个需要保护的主机上，只要部署在一个或多个关键访问点检测网络数据；即使黑客篡改了日志文件隐藏自己的痕迹，也

能检测出入侵，因为它捕获到的是网络上的数据流量；检测不依赖于主机的操作系统。NIDS 的缺点是：检测的精确度差；在交换和加密环境中难以部署。

2.2.3 入侵检测的标准模型 CIDF

目前针对 IDS 的规范化标准有两种[21]：一种是美国国防高级研究计划署(DARPA)制定的通用入侵检测框架(Common Intrusion Detection Framework,CIDF)，另一种是互联网工程任务组(IETF)的入侵检测工作组(Intrusion Detection Working Group,IDWG)建议草案。虽然这两种标准各自的出发角度不同，但都旨在解决不同 IDS 之间的共存和互操作问题。下面介绍其中 CIDF 标准。

CIDF[22]把一个入侵检测系统分为四个基本组件：事件产生器(Event Generators)、事件分析器(Event Analyzers)、响应单元(Response Units)、事件数据库(Event Databases)，如图 2-5 所示。

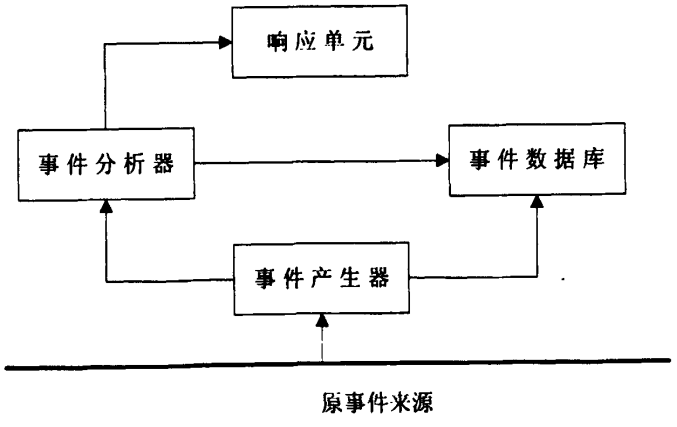


图 2-5 入侵检测系统 CIDF 模型

(1)事件产生器：其任务是从计算机环境中收集事件，并将这些事件转换成特定的格式传送给事件分析器和事件数据库。

(2)事件分析器：负责分析事件，并把分析结果交给事件数据库和响应单元。

(3)响应单元：对事件分析器分析的结果做出反应，如向管理员发出报警、切断连接、封锁 IP 等。

(4)事件数据库：事件数据库用来存储事件，以备查询和使用。

2.3 入侵检测技术的分析方法

入侵检测的分析方法主要有误用检测和异常检测。

2.3.1 误用检测技术

误用检测又叫做基于知识的（Knowledge-Based）检测。误用检测技术[23]是通过将预先设定的入侵模式与监控到的入侵发生情况进行模式匹配来检测。它假定所有可能的入侵行为都能被识别和表示。它需要预先建立一个包含过去各种入侵攻击的数据库，每种入侵攻击模式都用一种特定的方式表示，然后在通过收集和分析到的数据找到是否与数据库模式匹配的入侵攻击。误用检测不需要很高的系统条件，检测是通过模式匹配完成的，消耗资源少，并且有着较高的准确率，误报率低。误用检测技术以比较成熟。误用检测的不足在于不能检测未知的入侵行为，漏报率较高；依赖于操作系统,入侵数据库必须不断更新。下面列举几种不同的误用检测技术。

1.模式匹配法

模式匹配法 [23]是最常用的的误用检测方法，模式匹配模型在检测中根据待分析的事件在入侵模式数据库中搜索是否有对应的入侵模式，如果匹配成功，则判断为有入侵行为发生。这种方法的优点是易于实现，缺点是计算量大。模式匹配的算法的好坏决定了入侵检测系统的检测效果。

2.专家系统法

专家系统法是入侵检测方法中比较早的且的用的较多的一种检测方法，涉及人工智能领域。专家系统[24]是以专家的经验性知识为基础建立的，以知识库和推理机为中心的智能软件系统。在 MIDAS、IDES 和 NIDES 中，采用了该检测方法。

专家系统的优势是把系统的控制推理从问题的描述中分离出来，对已知入侵和系统漏洞检测的精确度高，通过更新不断增长应用领域，具有很大的灵活性。但它更新系统困难，系统开发的人为因素较大，面对海量信息时处理时间长，需要编写大量引擎和规则的代码。

3.状态转移分析法

状态转移分析法[25]使用高级状态转换图来体现和检测已知的入侵攻击方式。它将入侵行为看成是由攻击者执行的一系列行为操作组成，这些操作可将系统从某些初始

状态迁移到危及系统安全的状态。状态转移分析法的优点是比较直观，注重细节，非常适用于检测协同缓慢攻击。缺点是对引擎设计要求高，状态声明和信号动作需要手工编码。

2.3.2 异常检测技术

异常检测技术的假设条件是用户的行为是可以预测的，也被称为基于行为的(Behavior-Based)检测技术。异常检测首先建立系统历史正常活动的行为特征模式，然后将当前活动行为与之比较得出两者的差别程度。这个差别程度可以用阈值或一个范围衡量。当差别程度超出阈值或者一个范围，则判断为入侵行为。异常检测系统需要选取正常用户行为的特征量，建立一个正常行为模型，要求用尽可能少的特征量来描述正常的行为特征，因此特征量的选择是非常关键的。

异常检测技术的优势在于对未知的入侵行为的检测非常有效，能很好的检测假冒合法用户的入侵行为。劣势在误报率比误用检测高，建立行为模型时计算量大，对系统性能要求很高。按照不同异常检测方法，异常检测技术大致分为以下几种：

1.量化分析方法

量化分析法[26]的特点事务的特性用数值表示。它对加法和计算进行假设，然后进行完整分析和计算得出结果，最后根据结果建立预测模型。

2.统计分析方法

统计分析法是最早的异常检测方法。它的前提是假设系统正常的活动行为具有内在的统计规律。统计分析方法以统计数值作为基础，这些统计值由动态调节的参数控制。被检测的行为用一个经过计算得到的参数向量表示。对于用户所产生的每一个审计记录，系统经过计算生成一个单独的检测统计值，这个检测统计值用来表明最近用户行为的异常程度。统计分析方法是比较成熟的异常检测方法，但不足的是用统计分析方法形成的模型检测的入侵行为比较有限，阈值的确定有难度。

3.基于数据挖掘的检测技术

数据挖掘[27]能从计算机网络的大量审计记录和数据流中提取隐含的、事先未知的潜在有用的信息，提取的知识表示为概念、规则、规律、模式等形式。数据挖掘的过程由数据准备（包括数据选择和数据预处理）、数据挖掘、模式评估等几个部分组成。

数据挖掘技术不需要去手工分析和编写入侵模式，而且可以处理不同的数据源，

具有良好的可扩展性和自适应性。但基于数据挖掘技术的入侵检测系统需要开发有效的数据挖掘算法模型和体系结构来解决检测实时性差的问题。

4.基于朴素贝叶斯算法的检测技术

朴素贝叶斯算法[28]的数据源来自系统审计记录或网络数据流，在数据源中提取若干参数，如用户登录频度、CPU 占用率、系统调用命令次数等，把每个参数组成向量。朴素贝叶斯算法的是先从已知类别的训练集中得出先验概率，再计算出预测的后验概率，进而得出测试集中的类别。每一次计算出的后验概率后，可以作为下一次的先验概率继续计算，因此后验信息越来越接近真实值。

基于朴素贝叶斯算法的检测模型要求样本集比较全面，样本集需要不断更新，数据样本的特征之间必须相互条件独立。但由于其算法简单实用、计算高效、具有成熟的数学理论基础，因此在入侵检测中应用的较多。

5.基于人工神经网络的检测技术

人工神经网络[29]在 20 世纪 40 年代被第一次提出和建立，是人类在对其大脑神经网络认识理解的基础上用数学模型模仿大脑神经网络结构和功能的一种信息处理系统，后经过逐步的研究和发展，现广泛应用于自动控制、图像处理、模式识别和医学等领域。它由许多简单的元件通过某种关系相互连接而成，形成一个复杂的网络，有高度的复杂性和非线性，具有自适应性和自学习能力的特点。

6.基于遗传算法的检测技术

遗传算法是一个相比较而言复杂的事件数据分析算法。遗传算法吸收达尔文自然选择法则（适者生存）来解决问题。遗产算法在解决多维优化问题有很好的应用。在入侵检测处理中，遗传算法引入一个向量集和一个二次消耗函数，将一个特定攻击对系统的危险性乘以假设的向量值，然后由函数对结果调整，对不实际的假设进行删除。这样的结果是目标的结果被优化了。遗传算法目前在入侵检测系统中的应用主要有处理主机的信息和用处理用辅助手段获取信息两种情况。

2.4 入侵检测技术的发展趋势

2.4.1 入侵检测技术的现状

由于入侵检测是一项比较新的技术，因此在技术上存在一些困难，而且互联网的

技术更新太快，随之的入侵技术也要相应的做出改进，这对研究和开发人员提出了很大的要求。目前入侵检测产品还有以下几个方面的不足：

(1)检测系统的网络部署问题。随着网络规模的不断扩大，最初的只布置在网络的单节点处的集中式入侵检测系统很难满足用户的检测需求。现在大多数网络不再是小型的只有一个子网的小型网，而是有几个甚至几十个子网组成的大型网络。在网络中，有路由器、交换机、集线器和防火墙等网络设备，也有如 Web、FTP、DHCP、DNS、Telnet 等服务器，网络拓扑越来越复杂，网络设备之间的路由通信协议变化多样，因此对入侵检测的部署提出了新的挑战。

(2)用户隐私和网络管理问题。无论是基于主机还是基于网络的入侵检测系统，都能捕获到用户的通信数据包并分析保存，这对用户的隐私也就可能暴露了。

(3)网络数据量信息与实时响应问题。随着互联网技术的快速发展和普及，网络的带宽越来越宽，数据流量也在飞速的增长。入侵检测系统需要处理和分析大量的数据，并且尽可能的做到实时响应。

(4)入侵手段多样化问题。由于入侵手段能给入侵者带来很大的利益，所以现在入侵事件已非常普遍，入侵手段也层出不穷。目前除常见的入侵攻击如端口扫描、口令破解、拒绝服务攻击、病毒和木马外，还有新的一些入侵手段，如：超级蠕虫、隐秘多变代码攻击、路由和 DNS 攻击等。

(5)无线网络安全问题。近几年无线终端设备（手机、笔记本电脑等）的普及也使无线网络成了黑客攻击的新目标。由于无线网络加密系统的脆弱性，黑客很容易通过监听和欺骗得到关键数据。基于 802.11 标准的网络因为协议本身的缺陷，可能遭到拒绝服务攻击的威胁。

(6)与其它网络安全产品的兼容问题。因为网络结构时常有所变化，一整套网络安全产品可能来自不同厂家，不同厂家的产品可能会出现不能兼容的情况，这是需要考虑的问题。

2.4.2 入侵检测技术未来的趋势

随着对这个领域研究的不断深入，入侵检测技术的发展有三个方向[30][31]：

1.人工智能技术

人工智能是包括十分广泛的科学，研究的主要是使机器或系统能够完成一些需要

人类智能才能完成的复杂工作。它涉及数学、神经生物学、心理学、信息论和控制论等学科，研究范畴包括神经网络算法、数据挖掘、遗传算法等。神经网络具有很好的自学性，经过训练可以获得对入侵行为的预知能力，收敛性好，能提高检测率，可以检测一些新的攻击模式。尽管现在基于这方面技术的产品处在尝试阶段，但将来的前景值得期待。

2.分布式入侵检测技术

从目前的发展趋势来看，分布式的入侵检测系统是大的发展方向。集中式的入侵检测系统的中央控制节点一旦失效，整个入侵检测系统就失效。分布式技术能较好的解决这一问题。分布式的入侵检测系统分为主机代理、局域网代理和控制器三部分。主机代理主要分布在各主机上采集数据并传给控制器，局域网代理负责搜集局域网的数据信息并传给控制器，控制器用于分析数据进行入侵行为的判断。当控制器遭遇攻击失效时，各局域网代理就可以代替控制器进行网络数据的分析和入侵行为的判别。

3.IPS(Intrusion Prevention System)技术

IPS 即入侵防御系统，是一种全新的入侵防御系统，被称为高级入侵检测系统。IPS 克服了传统 IDS 最大的缺陷：对于大规模的分布式入侵攻击，传统 IDS 没有很好的检测效果，误报和虚警率较高，安全管理难度很大，而 IPS 有很好的解决方法并且能有效拦截入侵攻击。IPS 是一种智能的、主动的入侵检测系统，它不是简单地在恶意流量传送时或传送后才发出警报，而是预先拦截入侵攻击，这就能最大的避免入侵造成的损失。

IPS 的主要特征是：嵌入式运行模式、完善的安全策略、高质量的入侵特征库、高校处理数据包的能力和强大的响应功能。它的优势技术有：主动防御技术、同时拥有防火墙和 IDS 的功能、集成多种检测技术、基于硬件的加速系统。IPS 的这些优点，完全可以让人们相信它是 IDS 今后的发展趋势。

第3章 Kohonen和BP神经网络概述

3.1 人工神经网络介绍

3.1.1 人工神经网络发展历史

人工神经网络是用数学物理方法和信息处理手段对人脑神经网络进行抽象，建立起能模拟人脑功能和结构的智能系统。它是当今科学界人工智能研究领域内的一个热点。神经网络的发展历史大致分为三个阶段。

第一阶段从20世纪40年代到60年代末。1943年由心理学家麦克洛奇(McCulloch)和数学家皮斯(Pitts)在《Bulletion of Marhematical Biophysics》首次提出了神经元的数学模型，开启了神经网络研究的序曲，这个数学模型后被称为“M-P模型”。1949年赫布(Hebb)引入了突触的概念，提出了用突触来改变神经元连接强度的学习算法，现被称为“Hebb算法”[32]。1958年罗森布拉特(F.Rosenblatt)提出基于感知器(Perceptron)[33]模型的神经网络结构,并用计算机模拟实现，第一次将神经网络的研究付诸于实践，这是神经网络发展史上的一个的重大突破。20世纪60年代，由于数字计算机发展迅速，大量研究人员发现相比之下神经网络有很多缺陷转而投向数字计算机领域的研究。人工智能创始人明基斯(Minsky)和佩破特(papert)在1969年写的《Perceoirons》一书中指出基于感知器的神经网络智能解决简单的线性问题[34]，对于高阶谓词问题(如“异或”问题)毫无办法，至此神经网络的研究陷入低潮。

第二阶段从20世纪70年代初到1986年。1976年美国波斯顿大学的两位教授格罗斯贝格(S.Grossberg)和卡彭特(G.A.Carpenter)提出了非线性动力系统结构，推动了神经网络的发展研究。1982年美国加利福尼亚工学院教授霍普菲尔德(John Hopfield)提出了离散神经网络模型[35]，引入李雅普诺夫函数的概念，证明了该网络的稳定性，第一次将神经网络用于优化计算和联想记忆。这个理论的提出又使人们对人工神经网络产生了兴趣。1984年他又提出了连续神经网络模型，用运算放大器实现了神经元动态方程，并用电路实现了仿真，为神经网络的工程实现奠定了基础。随后的两年里，并行分布处理专家辛顿(Hinton)和鲁梅哈特(Rumelhart)相继提出了Boltsmann机和多层前馈网络的反向传播学习算法[36]。这个阶段，在许多科学家坚持

不懈的努力下，神经网络的研究摆脱了的困境，取得了不小的突破。

第三阶段从 1987 年到至今。1987 年在美国美国召开了第一届国际神经网络学术会议，在会上成立了国际神经网络学会(INNS)，将神经网络的研究工作推向了高潮。20 世纪 90 年代以后，涌现了许多专门研究神经网络的学术刊物，如：Neural Computation、Neural Networks、IEEE Transactions on Neyral Networks 等。1989 年我国在广州召开了全国第一届神经网络-信号处理会议，第二年在北京召开了第一届的神经网络学术大会。此后十几年，我国在人工神经网络的研究和实践方面都取得了令人可喜的成果，学术论文、研究人员和面向应用的工程技术人员也在逐年增加。目前，神经网络已广泛应用在模式识别、图像处理、语言处理、专家系统等领域，对人们的生活产生了巨大的影响。

3.1.2 人工神经网络的特点

人工神经网络可以按照不同的方法进行分类，如按照网络的结构分类，有前向网络和反馈网络；按照学习方式分类，有有监督学习和无监督学习网络；按照网络性能分类，有连续型和离散型网络等等。虽然人工神经网络有着几十种不同的模型，但它们都有共同的特点：

1.结构特点

神经网络的结构特点是具有分布存储信息和并行计算的能力。人工神经网络由大量简单处理元件相互连接构成，具有非线性且元件并行活动处理信息较快。神经网络将信息分布存储在所有神经元的连接权中，而不是只存在网络的某一部分中。正因为有了这样的存储结构，使得神经网络具有“联想记忆”的功能。神经网络能通过网络中预先存储的记忆进行训练，可以从部分信息或带有噪声干扰的信息中把原始的信息还原出来。

2.性能特点

神经网络的性能特点是有高度的非线性，良好的容错性。利用神经网络非线性，可以用来解决数学模型中复杂的非线性映射问题。因为神经网络信息的分布式存储，当网络中的一部分神经元不能正常工作时不会影响系统整体的功能。当输入模糊、残缺或变形的信息时，神经网络能通过联想记忆功能恢复完整的记忆，从而实现对不完整输入信息的正确识别。

3.能力特征

神经网络具有自适应的特征。所谓自适应，就是指系统能根据外界环境的变化而做出相应的改变。当外界环境发生变化时，经过一段时间的训练或感知，神经网络能通过自动调整网络结构参数，按照期望的输出调整神经元之间的连接权，逐步使输出达到期望目的。利用这个特征，神经网络可以用来样本的分类和识别。

3.1.3 人工神经网络的神经元模型

在生物神经学中，神经元是神经系统结构和功能的基本单位。大量神经元相互连接，构成了庞大和复杂的生物神经网络。神经元负责接收激励信号并做出兴奋或抑制的反应，神经元之间的强度随外部激励信息作自适应的变化，它是人脑信息处理的最小单元。人工神经元是对生物元的抽象描述，并用数学来建立模型来模拟生物神经元的结构和功能。人工神经元的原型是麦克洛奇(McCulloch)和数学家皮斯(Pitts)提出的M-P模型，后经过不断改进，形成了如图3-1所示的被广泛应用的模型[37]。

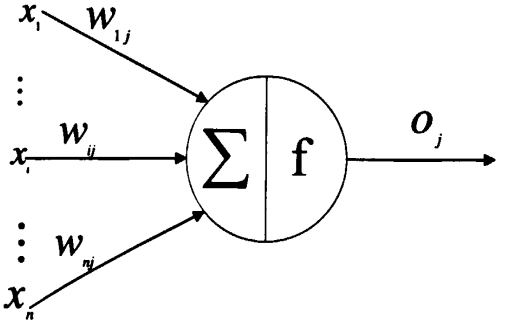


图3-1 神经元模型示意图

令$x_i(t)$表示t时刻神经元j接收的来自神经元i的输入信息，$o_j(t)$表示t时刻神经元j的输出信息，突触的时延取单位时间，则神经元j的状态可表达为：

$$o_j(t+1) = f\{[\sum_{i=1}^{n} w_{ij}x_i(t)] - T_j\} \tag{3-1}$$

其中T_j是神经元的阈值。w_{ij}是神经元i到j的连接权值，f( )是神经元的变换函数。如果令$x_0=-1$，$w_{0j}=T_j$，$W_j=(w_{1j},w_{2j},\cdots,w_{nj})^T$，$X=(x_1,x_2,\cdots,x_n)^T$，则$W_j^T X=\sum_{i=0}^{n} w_{ij}x_i$，神经元模型可简化为

$$o_j = f(W_j^T X) \tag{3-2}$$

不同的神经元数学模型其变换函数也不同，所以处理信息的特征也不同。变换函数的选取对神经网络整体的性能有着重大的影响。神经元的变换函数一般有四种：阈值型变换函数、非线性变换函数、分段线性变换函数和概率型变换函数。非线性变换函数中的单极性的 Sigmoid 函数曲线（简称 S 型函数），S 型函数的定义如下：

$$f(x) = \frac{1}{1+e^{-x}} \tag{3-3}$$

3.2 Kohonen 神经网络算法

3.2.1 Kohonen 神经网络的基本原理

Kohonen 神经网络[38]是由芬兰赫尔辛基(Helsink)大学的 T.Kohonen 教授提出的，是一种自组织竞争性网络。Kohonen 神经网络具有无监督、竞争识别分类的特点。脑神经学的研究表明，在脑的不同部位的神经细胞的分工不同，当大脑反复受到同一个外界的刺激时，大脑不同的部位的神经细胞反应不一，大脑皮层的某一处总是表现出特别兴奋。对于不同的输入模式，大脑皮层表现兴奋的有所部位不同。同时还发现，大脑中神经元的输入信号由整个神经网络的外部输入信号和同一区域的反馈信号组成，神经元之间交互信息的方式是：最相邻的两个神经元互相激励，较远的神经元相互抑制。两个神经元离的越近，能引起它们做出最大响应的频率就越接近。

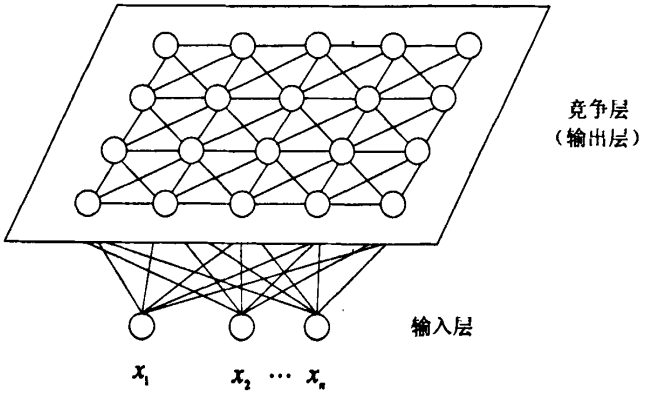


图 3-2　Kohonen神经网络模型

Kohonen 神经网络是两层结构的网络，由输入层和输出层构成。输入层是一维

的神经元，输入神经元数与输入样本维数相同。竞争层也就是输出层，竞争层上的神经元有多种排列方式，如一维线阵、二维平面阵和三维格栅阵，图3-2所示的就是二维阵列的Kohonen神经网络结构模型。

Kohonen神经网络的每个输入层神经元都与所有竞争层神经元通过权值连接起来，竞争层神经元相互之间可能也有连接。网络中有两种连接权值，一种是神经元对外部输入反应的连接权值，另一种是神经元之间的连接权值，后者的大小控制着神经元之间交互作用的强弱。邻近的神经元通过交互作用互相竞争，逐渐形成对输入模式的分类响应。Kohonen神经网络分训练学习和工作两个阶段。在网络学习阶段，输入一个样本时，神经网络将根据竞争层所有的神经元对应的输入向量与神经元内星权向量间欧几里德距离，比较两者的相似性，选择距离最小的神经元为获胜神经元。获胜神经元对其邻近神经元的影响由近及远从兴奋逐渐变为抑制，所以获胜神经元和其周围的神经元都要不同程度的调整权值。权值调整的方法是：以获胜神经元为中心设定一个邻域半径圈定一个范围，称为邻域。在这个领域内的所有神经元根据其距离获胜神经元的远近调整权值。调整方式一般用函数表示，常见的有墨西哥帽函数(图3-3(a))和大礼帽函数(图3-3(b))。墨西哥帽函数表明获胜神经元权值调整量最大，邻近的神经元离获胜神经元越远，调整量就越小，直到距离R后调整量变为0。当距离更远一点时调整量变为负的，表示抑制作用，再更远时到R'后又变为0，大礼帽函数也有与墨西哥帽函数相似的特点。优胜邻域在刚开始训练的时候定的很大，但随着训练次数的增加范围不断缩小，最终收缩到半径为0。

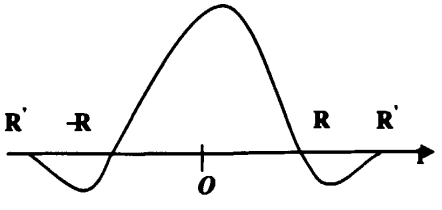


图3-3（a） 墨西哥帽函数

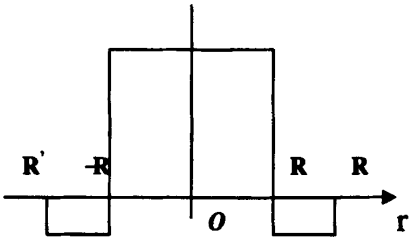


图3-3 (b) 大礼帽函数

通过大量样本的反复训练，神经网络通过自组织方式不断进行权值调整，最终各神经元的连接权值形成特别的分布，不同的神经元对特定输入模式类别敏感，当两个模式类的特征越接近，代表这两类的神经元在输出层网络上的位置也越近，权值也越

相近。Kohonen 神经网络在训练结束后，竞争层上就形成了对各种不同类模式的映射。当输入一个模式时，竞争层代表该模式类的神经元将产生最大兴奋，从而将该输入归为这一类。

3.2.2 Kohonen 算法的数学推导

Kohonen 神经网络训练算法的具体步骤如下：

(1) 网络的初始化

假设样本维数是 n 维的，则输入层节点数为 n,竞争层节点数为 m,输出层神经元连接权值赋予随机的小数，为 $w_{ij}(i=1,2,\cdots,n;\ j=1,2,\cdots,m)$，设其中一个训练样本的输入向量为 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$，令 $\boldsymbol{W}_j=(w_{1j},w_{2j},\cdots,w_{nj})(j=1,2,\cdots,m)$。首先对 $\boldsymbol{X}$ 和 $\boldsymbol{W}_j\ (j=1,2,\cdots,m)$ 进行向量归一化得到 $\hat{\boldsymbol{X}}$ 和 $\hat{\boldsymbol{W}}_j\ (j=1,2,\cdots,m)$，归一化按下式进行：

$$\hat{\boldsymbol{X}}=\frac{\boldsymbol{X}}{\|\boldsymbol{X}\|}=\left(\frac{x_1}{\sqrt{\sum_{j=1}^{n}x_j^2}},\cdots,\frac{x_n}{\sqrt{\sum_{j=1}^{n}x_j^2}}\right)^T \tag{3-4}$$

(2)寻找获胜神经元

分别计算输入模式向量 $\hat{\boldsymbol{X}}$ 和每一个神经元权向量 $\hat{\boldsymbol{W}}_j\ (j=1,2,\cdots,m)$ 的欧式距离 d_j

$$d_j=\left\|\hat{\boldsymbol{X}}-\hat{\boldsymbol{W}}_j\right\|=\left(\sum_{i=1}^{n}(w_{ij}-x)^2\right)^{1/2};\quad j=1,2,\cdots,m \tag{3-5}$$

从所有 d_j 中找出最小的值 d_{j^*}

$$d_{j^*}=\min_{j\in\{1,2,\cdots,m\}}d_j \tag{3-6}$$

d_{j^*} 值对应的第 j^* 个神经元为获胜神经元。

(3)定义优胜邻域 $N_{j^*}(t)$

以获胜神经元为中心确定 t 时刻的权值调整域，t 为训练次数。训练刚开始时 $N_{j^*}(0)$ 设定的较大，但随着训练时间 t 的增加，$N_{j^*}(t)$ 逐渐收缩，如图 3-4 所示。

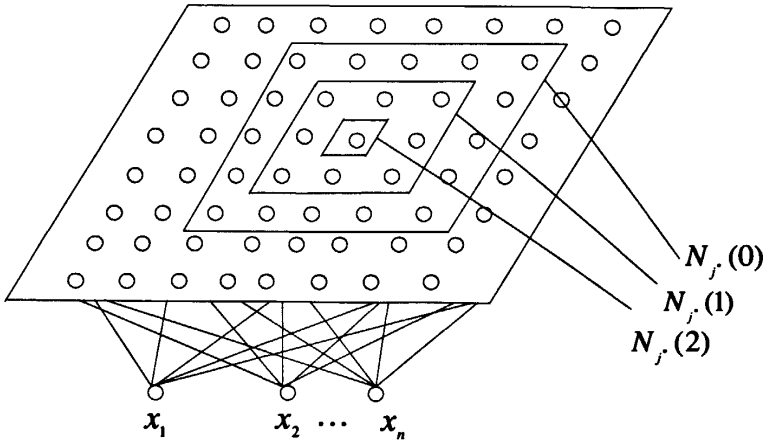


图 3-4 邻域的收缩过程

(4) 调整权值

权值的调整方法是对在优胜邻域内的神经元权值进行调整，不在优胜邻域范围内的不作调整

$$\begin{cases} w_{ij}(t+1)=w_{ij}(t)+\eta(t,N)[x_i-w_{ij}(t)] \ ,i=1,2,\cdots,n \quad j\in N_{j^*}(t) \\ w_{ij}(t+1)=w_{ij}(t) \ ,i=1,2,\cdots,n \quad j\notin N_{j^*}(t) \end{cases} \tag{3-7}$$

其中，$\eta(t,D)$ 是学习因子，范围 $0<\eta(t,D)<1$，它是训练时间 t 和第 j 个神经元与获胜神经元之间的欧式距离 D 的函数，一般与训练时间和欧式距离成反比。一般来说可把学习因子构造成如下函数

$$\eta(t,D)=\eta(t)e^{-N} \tag{3-8}$$

$\eta(t)$ 采用的是退火函数，所谓退火函数是指随时间单调下降的函数，图 3-5 给出了两种常用的退火函数。

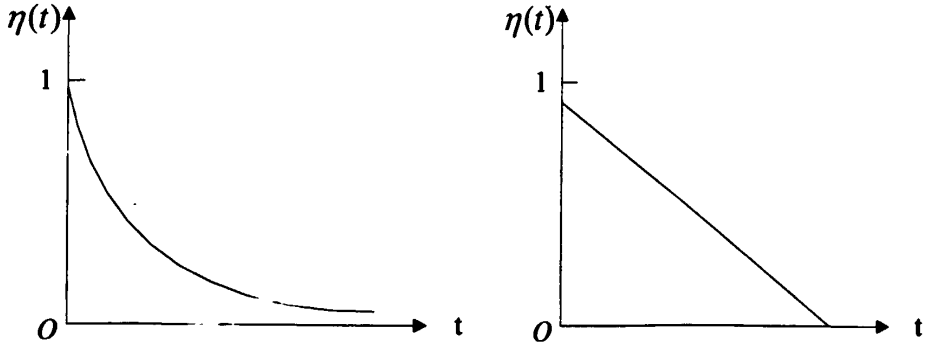


图 3-5　退火函数常见形式

(5)训练循环和结束

Kohonen 神经网络训练结束的标志是学校因子 $\eta(t,D)$ 衰减到某个比较小的正数或者零，若满足条件则训练结束，否则回到步骤(2)继续学习。

3.3 BP 神经网络算法

BP(Error Back Proragation)算法[39]即误差反向传播算法，由美国加利福尼亚的 PDP(Parallel Distributed Procession，平行分布式)小组提出，该算法是被多层感知器的训练采用的最多的算法，广泛应用在数据压缩、函数逼近、模式识别等领域。

3.3.1 BP 神经网络的学习过程

BP 神经网络的结构如图 3-6 所示。BP 神经网络有输入层、隐层和输出层三层，隐层可以有一个或多个，只有一个隐层的网络称为单隐层 BP 神经网络。

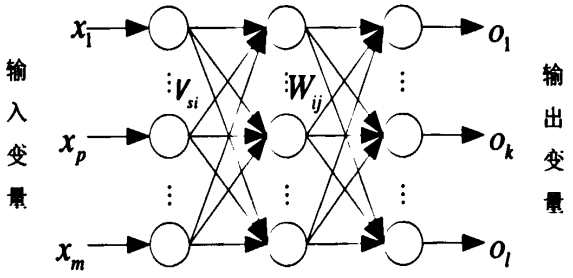


图 3-6　BP 神经网络结构

BP 神经网络是多层前馈网络的一种，采取有监督的学习算法，其同层网络的神经元之间没有任何连接，相邻的两层网络之间的神经元形成全连接。神经网络各层之间的连接权的作用是提取各层的输入向量特征和传递这些特征。网络的所有神经元的模型的输出函数都是非线性的。

神经网络的应用分为训练和工作两个阶段。在训练阶段，信号既要正向传播也要反向传播。在训练刚开始时，神经元之间的权值和阈值都是随机数，输入信号以向量形式从输入层输入，每个输入向量都有一个预期的输出向量对应，输入向量经过网络正向传播至输出层得到实际输出，再根据期望输出和实际输出的均方误差的梯度下降法调整各神经元之间的权值，调整的方向是从隐层向输入层反向传播，照这样不断的调整权值直到期望输出和实际输出的均方误差减小到零或一个很小的值。工作阶段是

在网络训练完成之后，对输入的模式进行分类，此阶段网络的权值是固定不变的。

3.3.2 BP算法的数学推导

BP算法的学习数学描述如下：

假设网络只有一个隐层，输入层有n个神经元，隐层有m个神经元，输出层有l个神经元，共有q个训练样本；输入层输入向量用 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)^T$ 表示，隐层输出向量用 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_m)^T$ 表示，输出层输出向量用 $\boldsymbol{O}=(o_1,o_2,\cdots,o_l)^T$，期望输出向量为 $\boldsymbol{d}=(d_1,d_2,\cdots,d_l)^T$；输入层到隐层间的连接权值为 w_{ij}，隐层到输出层的连接权值为 v_{jt}，隐层各神经元的阈值为 k_j，输出层阈值为 p_t $(i=1,2,\cdots,n;\ j=1,2,\cdots,m;\ t=1,2,\cdots,l)$；神经元变换函数为Sigmoid函数。

(1)网络初始化

给 w_{ij}，v_{jt}，k_j，p_t 赋予（-1,1）间的随机数作为初值。学习率 η 取0~1之间的小数。

(2)从q个训练样本随机选取一个样本输入网络，计算网络各层的输出

隐层和输出层的输出分别用以下公式表示：

$$y_j=f(\sum_{i=1}^{n}w_{ji}x_i-k_j)\qquad j=1,2,\cdots,m \tag{3-9}$$

$$o_t=f(\sum_{j=1}^{n}v_{ij}y_j-p_t)\qquad t=1,2,\cdots,l \tag{3-10}$$

(3)计算各层误差

输出层和隐层的误差分别用以下公式表示：

$$\sigma_t=o_t(1-o_t)(d_t-o_t)\qquad t=1,2,\cdots,l \tag{3-11}$$

$$\sigma_j=y_j(1-y_j)\sum_{t=1}^{l}v_{jt}\sigma_t\qquad j=1,2\cdots,m \tag{3-12}$$

(4)调整各层权值

设输入层与隐层之间的连接权值的调整公式：

$$\Delta w_{ij}=\eta x_i\sigma_j\qquad i=1,2,\cdots,n;\quad j=1,2,\cdots,m \tag{3-13}$$

$$\Delta v_{jt} = \eta y_j \sigma_t \quad j = 1,2,\cdots,m; \quad t = 1,2,\cdots,l \tag{3-14}$$

(5)将训练样本数减1，回到步骤(2)，直到q个样本训练完为止。

(6)全部样本训练完一次后，计算网络的输出，若误差不满足要求，则继续用样本训练直到误差满足要求为止。

BP神经网络实现了一个输入-输出的模式映射的功能，而在这之前并不清楚这种映射关系。它能够解决一些难以用数学方法描述规律的问题。BP网络具有泛化能力，网络通过样本学习逐渐形成非线性映射关系并把这些关系存储记忆在权值中，在工作阶段，网络能够对未曾碰到过的样本做出正确的映射。BP网络还具有容错能力，因为是经过提取大量样本的统计特征后才会做出对网络权值的调整，所以个别有较大误差的输入样本不会对网络的学习过程造成影响。

3.4 神经网络在入侵检测中的应用

人工神经网络具有分布存储信息和并行计算的特点，拥有高度的非线性映射的能力和自适应性，良好的容错性，这些条件使其应用在入侵检测系统中变成了可能。利用神经网络的学习能力，入侵检测系统能从系统网络数据流和审计日志中提取正常用户行为和入侵行为的模式特征。神经网络预先要经过训练，需要准备训练用的分类数据集。训练集包含正常分类数据和异常分类数据，且用特定的符号表示，如可用“0”表示正确数据，"1"表示异常数据，然后控制分类器的输出进行训练。神经网络的自学能力使它能够在训练中逐步自动构造出一个分类器网络来区分正常数据和异常数据。神经网络具有强大的学习和分类能力，它很好的利用了数据特征间的各种相关性，把入侵检测看成是一个模式分类的过程，尽管现今还只停留在理论研究上面，但其在它必定在将来成为入侵检测技术应用领域中的热点。

第 4 章 入侵检测系统的设计

4.1 系统的总体设计

在入侵检测系统的设计过程中，应该遵从模块化的原则[40]。所谓模块化，是指将一个复杂的问题按照某种原则系统地划分为若干个具有不同功能的模块。将入侵检测系统分成若干个子模块，有利于将复杂的问题简单化，这样既容易在设计中找到问题的出处，又使后期系统的更新和维护变的方便。

一个入侵检测系统的设计要求包括：满足用户最基本的检测需求，能实时检测入侵行为，能及时更新系统。根据以上要求设计的入侵检测系统结构如图 4-1 所示。

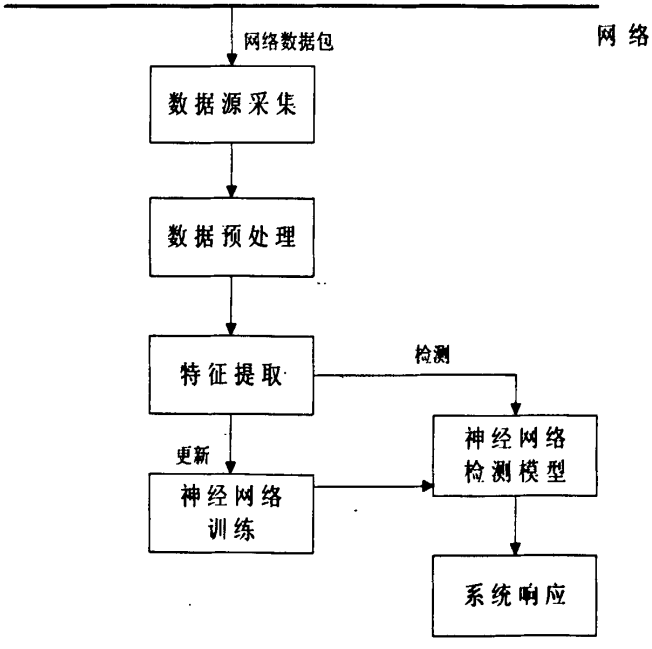


图 4-1　入侵检测系统的体系结构

该系统结构分成六大模块：数据源采集模块、数据预处理模块、特征提取模块、神经网络训练模块、神经网络检测模块和系统响应模块。数据源采集模块主要负责监听网络接口，捕获经过的数据包，并过滤数据包得到系统需要的数据。数据预处理模块主要负责将数据包的特征信息转换到一个标准的向量空间。特征提取模块主要负责消减数据的特征维数，提高系统的处理速率。神经网络训练模块负责系统的训练工作。

神经检测模块主要负责系统的入侵检测工作。系统响应模块根据检测模块返回的信息对用户行为作出响应。

4.2 数据源采集模块

本设计采用的是基于 Libpcap 的数据包捕获机制采集网络中的数据包。Libpcap[41](Packet Capture Library)是 Unix/Linux 平台下的一个数据包捕获函数库，在 Windows 平台下称为 Winpcap。网络上的许多有名嗅探器如 sniffer 和 snort 都是基于 libpcap 开发的。利用 Libpcap 提供的函数库，就可以通过网卡抓取网络中的数据包。Libpcap 的函数库为不同的平台提供了统一的 API 接口，而且结构简单，能在多个操作系统上使用，非常方便。

Libpcap 的通过将网卡设置为混杂模式来实现对整个网络上的数据包的捕获。网络驱动程序对捕获到的数据包和系统发送的数据包进行拷贝，把拷贝的部分送到内核中的数据包过滤模块，过滤模块依照系统设置的过滤条件对数据包进行过滤，再交给数据预处理模块。上述的这种包捕获机制称为 BPF[41]，如图 4-2 所示。在整个数据包的捕获和过滤过程中，BPF 并不影响操作系统对数据包的正常协议栈处理。

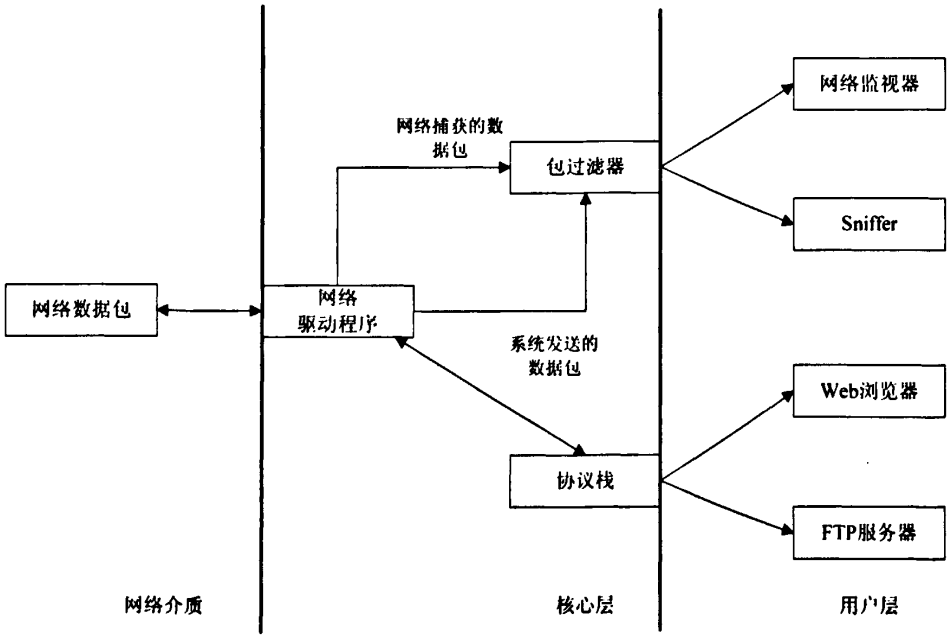


图 4-2　BPF 包捕获机制

4.3 数据预处理模块

4.3.1 数据预处理模块功能

数据源采集模块抓取的数据大多是含有噪声的、不完整、不一致的低质量数据，无法送入特征提取模块进行处理，也无法被神经网络训练模块或检测模块识别。为了提高数据的质量和系统的处理效率，使数据保持一致性，必须经过数据预处理过程。本设计的数据预处理模块的工作主要包括数据清理、数据集成和变化、数据规范化[42]三个过程。

数据清理目的是将数据中的噪声和无关数据去掉并且消除数据的不一致现象。数据清理的办法有：填补遗漏数据、平滑噪声数据、消除异常数据、填充空值等。

数据集成和变换就是在信息处理之前将涉及多个数据源的海量数据集进行合并存储，对不适合信息处理的数据进行变换。数据集成需要将来自不同数据源的数据进行整合，然后以统一的形式存储，常用方法有模式集成和删除冗余等。数据变换有平滑、聚集和数据概化这几种方法。

数据规范化就是把描述信息的多个属性统一起来，得到一个综合指标，进而对数据做一个整体上的评价。常见的方法有最小-最大规范法、零-均值规范化和小数定标规范化。

4.3.2 实验数据集

本实验使用的数据的来源是 KDD99 数据集。KDD99 数据集[43]出自美国麻省理工(MIT)的林肯实验室，美国国防部高级规划署(DARPA)为了开展一项入侵检测评估项目而开发出了这个数据集。林肯实验室[44]模拟了美国空军局域网的环境，该环境就像真实的网络环境一样，期间使用了各种不同的网络攻击和入侵手段，并且采集了 9 周时间的 TCPdump(*)系统审计和网络连接数据。KDD99 数据集分为训练集和测试集两部分。训练集是 7 星期的 5 百多万条网络连接记录，测试集是 2 星期的 2 百多万条网络连接记录。

数据集共包含 22 种入侵行为，分为四大类：

(1)拒绝服务攻击(Denial of Service Attacks,DoS)

拒绝服务攻击大致分为三类[45]：一类是由于软件漏洞或者错误配置造成的；一类是因为协议漏洞引起的，如 teardrop 攻击；另一类是通过合理的服务请求大量消耗服务器资源，导致系统无法对其它要求作出响应。数据集中属于 DoS 的入侵行为有：land、back、neptune、pod、smurf、teardrop。

land 攻击的特征是发送数据包的源 IP 和目标 IP 相同，源端口和目标端口也相同，致使计算机系统无法处理大量这样的数据包而死机。back、neptune 攻击的方法与其相似。

pod 攻击的全称是 ping of death，该攻击的特征是在短时间内发送大量的超过 64KB 的 ICMP 报文，当计算机系统处理这样大的数据包时，会导致内存分别错误和 TCP/IP 协议栈溢出。

smurf 攻击的特征是：主机 B 冒充主机 A 的 IP 地址向某一网络发送的大小为 1K 的 Ping 广播包，如果该网段有 10 万台主机，那么主机 A 将收到大 100M 的回应包，如果主机 B 冒充主机 A 不停的发送这样的数据包，那么主机 A 的网络资源会遭到大量的消耗而无法对其它主机提供服务。

Teradrop 攻击利用的是主机在处理数据包分片时的漏洞。它的攻击特征是向主机发送大量错误的数据包分片，这样导致 IP 协议栈的破坏，主机只能重启才能恢复。

(2)探测攻击(Probing)

探测[45]是入侵者在攻击之前展开的情报收集工作，主要是利用各种入侵工具盒技巧，对攻击目标进行扫描和查点，以便找到目标的安全弱点。收集工作的主要内容包括：DNS、邮件等服务器的 IP 地址和名称，攻击目标网络的拓扑结构等。扫描一般是通过 Ping、端口扫描工具 nmap 和 netcat、安全漏洞扫描工具 Scanner 和 nessus 等。数据集内的探测攻击有：ipsweep、nmap、portsweep 和 satan。

ipsweep 攻击又称 IP 扫描，它是一种简单的网络地址扫描方式，通过发送 ICMP 回应请求到某一地址段的所有主机，根据响应情况分析被扫描网络及主机的基本情况。

nmap 攻击的原理与 ipsweep 类似，只不过 nmap 支持 TCP、UDP、ICMP、FIN、ACK 等多种扫描技术。

portsweep 和 satan 攻击主要运用的是 TCP / UDP 的扫描技术、扫描的目标主要是计算机或服务器的开放端口或端口漏洞，且都用于远程扫描。

(3)未授权的本地超级用户特权访问(unauthorized access to local superuser privileges by a local unpivileged user,U2R)

U2R 攻击是指入侵者在已获得系统普通用户权限的情况下，利用操作系统的漏洞获取系统更高的权限的攻击方法。这里的操作系统可以是 Linux、Unix 系统的、也可以是 Windows NT、Windows Server 系列的。数据集中属于 U2R 攻击的有：buffer_overflow、loadmodule、perl、rootkit。

buffer_overflow 称为缓冲区溢出攻击。操作系统的缓冲区又叫堆栈，用于临时存放各进程间的操作指令。在正常情况下，程序都会认为数据长度能与所分配的存储空间匹配，但一旦程序的长度超过缓冲区的长度，就会发生堆栈溢出。入侵者就是利用这一缺陷，使程序的函数返回时跳转到任意地址导致系统服务拒绝。

loadmodule 和 perl 攻击的手法类似，利用的是系统的格式化字符串漏洞，将预先编好的恶意脚本注入系统，从而获得系统的高级权限。rootkit 是黑客取得主机管理员权限并能清除自己入侵行踪的工具。

(4)来自远程主机的未授权访问(unauthorized access from a remote machine to a local machine，R2L)

R2L 攻击是指入侵者在没有目标主机账号的情况下，通过远程攻击取得目标主机的访问权限的入侵方法。数据集中的 R2L 攻击有：ftp_write、guess_passwd、imap、multihop、phf、spy、warezclient、warezmaster。以下仅举有代表性的 imap、phf、spy 和 guess_passwd。

imap 攻击是利用 IMAP 协议（交互式邮件存取协议）的漏洞进行入侵的。这个漏洞是 IMAP 服务在处理一些指令时忽略了边界的检查，如果用户的指令的长度达到一定值，就会造成缓冲区溢出。

phf 攻击是针对浏览器的攻击。pdf 攻击利用了 Apache Web 服务器的一个脚本文件的漏洞，使攻击者通过分析验证信息来获取服务器用户的特权。

spy 攻击的方法是在用户浏览网页、查看邮件、下载资料时在主机中植入间谍软件和木马，黑客通过间谍软件和木马来盗取主机的重要信息，甚至能远程控制主机。

guess_passwd 是利用 John 分析法、在线猜测系统和非字典算法等方法来破解 Telnet、SSH、E-mail 等服务器的登陆密码。

KDD99 数据集的数据形式如表 4.1 所示：

表 4.1KDD99 数据形式

0,tcp,http,SF,222,773,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,11,11,0.00,0.00,0.00,0.00,1.00,0.00,0.00,38,129,1.00,0.00,0.03,0.04,0.00,0.00,0.00,0.00,normal.
0,tcp,ftp_data,SF,0,467968,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,2,2,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.00,multihop.
0,icmp,ecr_i,SF,1032,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,511,511,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,255,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.00,smurf.
0,tcp,smtp,SF,93005,403,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,2,0.00,0.00,0.00,0.00,1.00,0.00,1.00,7,2,0.29,0.43,0.14,0.00,0.14,0.00,0.00,0.00,normal.

数据集的每条数据都有 42 个特征[41]，最后一个特征用来注明该条数据是正常还是某种攻击类型，前面的 41 个特征是可以归为 4 大类，如表 4.2 所示。每一行数据特征的1~9列为TCP连接的基本特征；第10~22列为TCP连接的内容特征；第23~31列为过去两秒内的网络流量统计特征；第 32~41 列为过去两秒内的主机的网络流量统计特征。

表 4.2 KDD99 数据集特征描述

列号	特征名	特征描述	类型
1	duration	连接持续的时间(s)	连续
2	protocol_type	协议类型	离散
3	service	目标的网络服务	离散
4	flag	网络连接的状态，正常或错误	离散
5	src_bytes	从源地址到目标地址的字节数	连续
6	dst_bytes	从目标地址到源地址的字节数	连续
7	land	源和目的主机的 IP 或端口相同，相同为 1，否则为 0	离散
8	wrong_fragment	错误分片的数据包数目	连续
9	urgent	tcp 控制字段标记为 urgent 的紧急包数目	连续
10	hot	“hot”指针的数目	连续
11	num_failed_logins	尝试登陆失败的次数	连续
12	logged_in	登陆成功为 1，否则为 0	离散
13	num_compromised	“compromise”条件的次数	连续
14	root_shell	取得 root shell 的为 1，否则为 0	离散
15	su_attempted	是否尝试用 su root 命令，如果是为 1，否则为 0	离散
16	num_root	以 root 身份访问的次数	连续
17	num_file_creations	建立文件操作的次数	连续
18	num_shells	Shell 提示的次数	连续
19	num_access_files	对访问控制文件的操作次数	连续

20	num_outbound_cmds	在一个 FTP 会话中使用的命令数	连续
21	is_hot_login	本次登陆是否属于 hot 列表，如果是为 1，否则为 0	离散
22	is_guest_login	本次登陆是否是 guest 登陆，如果是为 1，否则为 0	离散
23	count	过去两秒内，与当前连接具有相同的目标主机的连接数	连续
24	srv_count	与当前连接具有相同服务的连接数	连续
25	serror_rate	在与当前连接具有相同目标主机的连接中，出现“SYN” 错误的连接的百分比	连续
26	srv_serror_rate	在与当前连接具有相同服务的连接中，出现“SYN” 错误的连接的百分比	连续
27	rerror_rate	在与当前连接具有相同目标主机的连接中，出现“REJ” 错误的连接的百分比	连续
28	srv_rerror_rate	在与当前连接具有相同服务的连接中，出现“REJ” 错误的连接的百分比	连续
29	same_srv_rate	与当前连接具有相同服务的连接的百分比	连续
30	diff_srv_rate	与当前连接具有不同服务的连接的百分比	连续
31	srv_diff_host_rate	与当前连接具有不同目标主机的连接的百分比	连续
32	Dst_host_count	对同一目标主机的连接数	连续
33	Dst_host_srv_count	与当前连接具有同样服务的连接数	连续
34	Dst_host_same_srv_rate	与当前连接具有相同服务的连接数百分数	连续
35	Dst_host_diff_srv_rate	与当前连接服务不同的服务连接百分数	连续
36	Dst_host_same_src_port_rate	与当前同一端口的连接所占百分比	连续
37	Dst_host_srv_diff_host_rate	与当前同一服务不同源主机的连接百分数	连续
38	Dst_host_serror_rate	具有 S0 错误连接的百分数	连续
39	Dst_host_srv_serror_rate	与当前同一服务且有 S0 错误的连接的百分数	连续
40	Dst_host_rerror_rate	具有 RST 错误的连接百分数	连续
41	Dst_host_srv_rerror_rate	与当前同一服务且有 RST 错误的连接的百分数	连续

4.3.3 实验数据集的预处理

在 KDD99 数据集中，有部分特征的值为离散值，如第三列特征 service 的取值是字符，分别有 tcp、udp 和 icmp 三种类型，为了使它们被神经网络识别，分别用数值 1、2 和 3 代替。其余离散变量也用相似的方法进行处理。此处理过程是用 python 处理语言完成的。

离散化的变量处理完后，需要进行数据的标准化。标准化采用如下方法：

(1)计算特征变量属性的平均值

设有 M 个样本，x_{ji} 是第 j 个样本的第 i 个特征的值，A_i 是第 i 个特征的平均值，则：

$$A_i = \frac{1}{M}\sum_{j=1}^{M} x_{ji} \tag{4-1}$$

(2)计算样本特征的均方差

设第 i 个特征的均方差为 C_i 公式如下：

$$C_i = \sqrt{\frac{1}{M-1}\sum_{j=1}^{M}(x_{ji} - A_i)^2} \tag{4-2}$$

(3)归一化

归一化后新的特征值 x_{ji}^* 为:

$$x_{ji}^* = \frac{x_{ji} - A_i}{C_i} \tag{4-3}$$

4.4 特征提取模块

现今的网络数据流量日益增长，对入侵检测的处理速度提出了很高的要求。KDDUP 数据集中数据的特征有 41 个，维数比较高，各特征之间存在着较大相关性，若直接送至训练或检测模块，数据的计算量很大，可能影响 IDS 的检测速度和响应速度。特征提取[46]就是从一组度量值 $(x_1, x_2, \cdots, x_L)$ 通过某种变换 $h_i(\bullet)$ 产生新的 m（m<L）个特征 $(y_1, y_2, \cdots, y_m)$ 作为降维的分类特征，其目的是保证在一定分类精度的前提下，尽可能保留分类信息，减少特征维数，使分类器既快速又准确。目前，特征提取主要采用的方法有主成分分析（Principle Component Analysis,简称 PCA）[47]、核主成分分析（KPCA）、和非线性成分分析法等。本设计采用的是主成分分析提取技术，主成分分析的优点是高效和简单易用，广泛应用于图像处理、文本分析、语音识别等领域。

4.4.1 主成分分析的基本原理

主成分分析[48]就是设法将原来众多具有一定相关性的指标（比如 p 个指标），重新组成一组新的相互无关的综合指标来代替原来的指标，达到降维的目的。新组成

的综合指标的个数比原指标少，称为“主成分”，主成分能够反映原来指标的绝大部分信息。利用主成分分析技术可以减小消除原指标之间的相关性和冗余信息，减小后续工作的计算量。

设有样本为 n，样本的特征数为 p，x_{rs} 为第 r 个样本的第 s 个特征值 $(r=1,2\cdots,n;s=1,2,\cdots,p)$，令 $X_i=(x_{1i},x_{2i},\cdots,x_{ni})^T\ (i=1,2,\cdots,p)$，则总样本矩阵 X 可用 p 个列向量表示：

$$X=\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1p} \\ x_{21} & x_{22} & \cdots & x_{2p} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{np} \end{bmatrix}=(X_1,X_2,\cdots,X_p)$$

这里设：

$$F_i=a_{1i}X_1+a_{2i}X_2+\cdots+a_{pi}X_p \qquad i=1,2,\cdots,p \tag{4-4}$$

$$a_{1i}^2+a_{2i}^2+\cdots a_{pi}^2=1 \qquad i=1,2,\cdots,p$$

其中，F_i 是 $X_1,X_2,\cdots,X_p$ 的一切线性组合，F_i 与 $F_t\ (i\neq j,i,t=1,2,\cdots,p)$ 不相关。

令 $a=(a_{11},a_{21},\cdots,a_{21})$，$V=X^T$

$$F_i=a_{1i}X_1+a_{2i}X_2+\cdots+a_{pi}X_p=a^TV \tag{4-5}$$

求主成分就是寻找 V 的线性函数 a^TV 使相应的方差尽可能的大，即使 $Var(F_1)=Var(a^TV)=E(a^TVV^Ta)=a^TE(XX^T)a$ 达到最大值，且 $a^Ta=1$。令 $W=E(VV^T)$，则 $Var(F_1)=a^TWa$。

设 W 的特征根为 $\lambda_1,\lambda_2,\cdots,\lambda_p$，不妨假设 $\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_p>0$，相对应的单位特征向量为 $u_1,u_2,\cdots,u_p$，令 $U=(u_1,u_2,\cdots,u_p)$。由于 $W=\sum_{i=1}^{p}\lambda_iu_iu_i$，因此

$$a^TWa=\sum_{i=1}^{p}\lambda_ia^Tu_iu_i^Ta=\sum_{i=1}^{p}\lambda_i(a^Tu_i)(a^Tu_i)^T=\sum_{i=1}^{p}\lambda_i(a^Tu_i)^2 \tag{4-6}$$

所以

$$a^T W a \le \lambda_1 \sum_{i=1}^{p} (a^T u_i)^2 = \lambda_1 (a^T U)(a^T U)^T = \lambda_1 a^T U U^T a = \lambda_1 a^T a = \lambda_1 \quad (4\text{-}7)$$

可以证明[4]，当$a = u_1$时使$Var(F_1)$达到最大值。

第 i 个主分量的贡献率定义为：

$$\lambda_i / \sum_{i=1}^{p} \lambda_i \qquad (i = 1,2,\cdots,p) \quad (4\text{-}8)$$

而前 m 个主分量的累计贡献率定义为[48]

$$\sum_{i=1}^{m} \lambda_i / \sum_{i=1}^{p} \lambda_i \quad (4\text{-}9)$$

若F_1无法足够多的代表原始数据时，主要体现在其主分量贡献率（$\lambda_1 / \sum_{i=1}^{p} \lambda_i \ (i = 1,2,\cdots,p)$）未达到一定要求的情况下，需要进一步提取其它的主成分，即需要进一步得到出$(X_1, X_2, \cdots, X_p)$线性组合形成的$F_i \ (i = 1,2,\cdots,p)$。此时的得出的F_i必须满足：

(1)与之前得出的所有主成分分量$F_j (j < i)$线性无关

(2)方差最大

与推出F_1的原理类似，可得出以下的结论：当$a = u_2$时使F_2满足上述要求，当$a = u_p$时使F_p满足上述要求。

在解决实际问题时，当累计贡献率满足一定的要求(一般在 85%以上)的 m 的值就是主成分分量的个数，这些主成分用来代替原数据指标来反映数据的信息，一般情况下$m < p$。本设计取满足 90%以上贡献率的主成分分量。

4.4.2 主成分分析的计算步骤

(1)设有样本为 n，样本的特征数为 p，x_{rs}为第 r 个样本的第 s 个特征值$(r = 1,2\cdots,n; s = 1,2,\cdots,p)$，计算样本的协方差矩阵：

$$C_x = \mathrm{cov}(X) = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1p} \\ C_{21} & C_{22} & \cdots & C_{2p} \\ \vdots & \vdots & & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{pp} \end{bmatrix} \tag{4-10}$$

其中，$C_{ij} = \dfrac{\sum_{k=1}^{n}(x_{ki}-\overline{x_i})(x_{kj}-\overline{x_j})}{\sqrt{\sum_{k=1}^{n}(x_{ki}-\overline{x_i})^2(x_{kj}-\overline{x_j})^2}}$，$\overline{x_d} = \dfrac{1}{n}\sum_{t=1}^{n} x_{td}\ (i,j,d = 1,2,\cdots,p)$。

(2)计算特征值与特征向量：

利用特征方程$|\lambda I - C_x| = 0$，求出特征值λ_i和对应的特征向量e_i，其中特征值满足，$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_p \geq 0, i = 1,2,\cdots,p$。

(3)按式(4-8)和(4-9)计算各分量的贡献率，并根据需要选取前 m 个$(m < p)$个分量作为主分量。

4.5 神经网络训练和检测模块

神经网络训练和检测模块是入侵检测系统的核心。当入侵检测系统处在训练模式时，将数据放入训练模块对神经网络进行训练，提高网络对入侵的识别率。当入侵检测系统处在检测模式时，检测模块对数据进行检测识别入侵行为。这里主要讨论基于 Kohonen 神经网络和 BP 神经网络的入侵检测系统。

4.5.1 Kohonen 神经网络的设计

选取 KDD99 数据集中具有 41 个特征的数据，经过数据预处理和 PCA 特征提取，进入 Kohonen 网络。网络分训练和检测两个阶段。在训练阶段，Kohonen 网络的神经元根据训练数据的已知向量的对应关系贴上标签，竞争层得出各模式的最强响应的神经元。在检测阶段，神经网络的神经元将检测数据产生的响应神经元与训练得到的响应神经元进行比较进而分类。

(1)网络初始化

在训练前，需要对网络的各参数进行初始化。如果是经过了 PCA 特征处理过后的数据，输入层神经元的数目和处理后的数据维数相同。对于竞争层的节点数，既不

能太多，也不能太少，本设计选取 6×6 的二维平面节点，即一共 36 个神经元。网络的初始权值为 0～1 之间的随机数。

(2) 优胜邻域的设计

优胜邻域的设计原则是邻域半径随训练次数的增加而不断缩小，这样就能保证最大响应的获胜神经元相邻的神经元取得比较大的兴奋。

设优胜邻域为 r(t)，最大邻域为 r_{max}，最小邻域为 r_{max}，总学习次数为 m，t 为训练次数，本设计使用如下邻域计算公式：

$$r(t)=\frac{(r_{\max}-t)(r_{\max}-r_{\min})}{m} \tag{4-11}$$

其中，r_{max} 取值为 1.5，r_{min} 取值为 0.8，m 取值为 6000。.

(3)学习率的设计

学习率决定着权值调整的速度，在刚开始训练的时候，学习率应该取大点的值，以便快速对网络的大致结构进行定位。在训练过程中，学习率缓慢下降直至最后趋于零，这样可以达到精确调整权值的大小，使网络的结构更加准确的对输入进行反应。

设学习速率为 rate(t)，最大学习速率为 $rate_{max}$，最小学习速率为 $rate_{min}$，总学习次数为 m，t 为训练次数，本设计使用如下学习率计算公式：

$$rate(t)=\frac{(rate_{\max}-t)(rate_{\max}-rate_{\min})}{m} \tag{4-12}$$

其中，$rate_{max}$ 取值为 0.2，$rate_{min}$ 取值为 0.05，m 取值为 6000。

4.5.2 BP 神经网络的改进和设计

4.5.2.1 BP 算法的不足和改进

1.BP 算法的不足

虽然传统的 BP 网络应用广泛，取得了很多实际成果，但它还是存在着许多固有的缺陷，具体如下：

(1)BP 算法学习速度慢

BP 算法实质上是梯度下降算法的一个应用。BP 网络的误差函数可以用函数表示：

$$E=F(W,V) \tag{4-13}$$

W、V 是网络的权值矩阵。图 3-7 是 $E = F(w_{11}, w_{12})$ 的二维误差曲面图形。

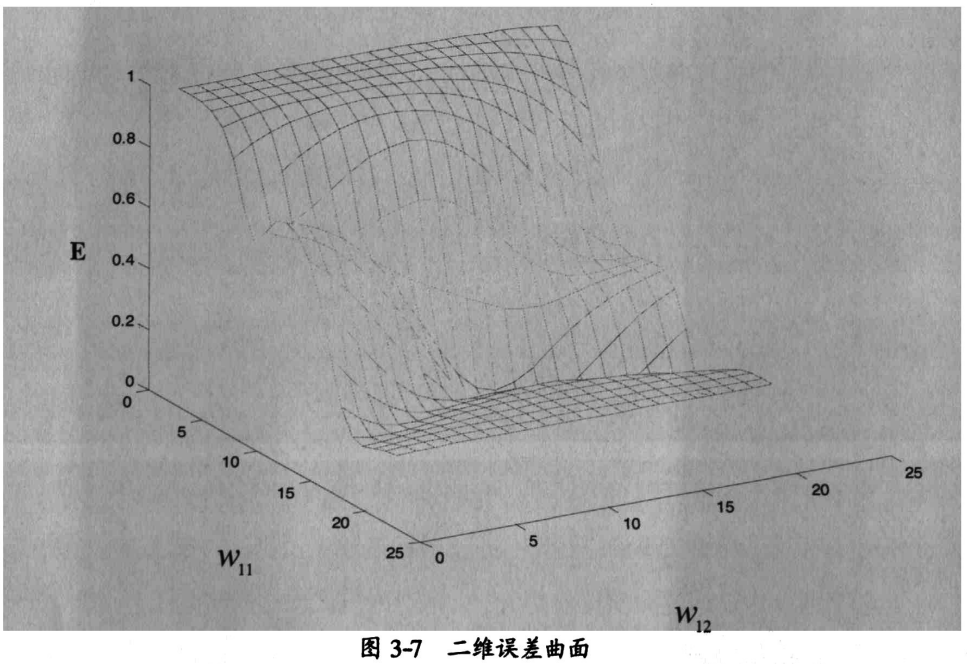


图 3-7　二维误差曲面

在网络的误差[29]曲面上存在一些平坦的区域，训练进入平坦区域后，如果输出与预期相差任然很大，但由于误差的梯度变化很小，权值调整量很小，将导致训练次数大大增加，网络的学习速度变慢。但是只要权值的调整方向正确，误差总可以离开平坦区。

(2)BP 网络训练无法收敛

误差曲面的低谷区就是误差函数的极小点。在多维空间中误差曲面有很多的极小点，无论是全局极小点还是局部极小点，误差梯度都为零。在训练时，基于梯度下降法的 BP 算法得到的使网络权值收敛的点可能是一个局部极小点。由于 BP 算法[37]无法区别极小点的性质，因此网络常常无法逃出局部极小点而使训练无法收敛。

2.BP 算法的改进

针对传统 BP 算法出现的上述问题，人们提出了不少改进的算法。以下是一些常用的方法[49]-[51]：

(1)附加动量法

附加动量法的思想是：把 t-1 时刻的梯度方向引入到 t 时刻误差梯度下降方向调

整中，从而减小网络学习过程中的震荡趋势，加快收敛速度。在原有的梯度下降法的基础上增加一项动量项，动量项与前一次的权值变化量成正比。将公式(3-13)和(3-14)分别调整为：

$$\Delta w_{ij}(t+1)=(1-m_{c1})\eta x_i\sigma_j+m_{c2}\Delta w_{ij}(t) \tag{4-14}$$

$$\Delta v_{jt}(t+1)=(1-m_{c2})\eta y_j\sigma_t+m_{c2}\Delta v_{jt}(t) \tag{4-15}$$

其中，t为训练次数；m_{c1},m_{c2}为动量因子，一般有$m_{c1},m_{c2}\in(0,1)$。

加入动量项后，当前一次权值的调整量过大时，本次的权值调整量就会减小从而避免网路发生振荡。当前一次权值的调整量过小时，本次的权值调整量就会适当地增大，这样有助于网络从误差曲面的局部极小值中跳出。

(2)自适应学习速率法

在传统的BP算法中学习率η为常数，但在实际运用时，很少能找到一个自始至终都适当的学习率，使其能够把权值调整到最佳。通过误差曲面可以发现，如果一开始选择的学习率太小，当遇到平坦区域时就会使训练次数增加；如果一开始选择的学习率太大，遇到误差变化较大的区域训练会出现振荡减缓网络的收敛速度。解决这个问题办法是在训练中自适应地调整学习率。调整学习率的思路是：当调整后的权值能降低误差函数并接近目标时，说明此时的学习率偏小，适当地给学习率增加一个量；当出现与上面相反的情况时，适当地减小学习率的值。调整公式如下：

$$\eta(t+1)=\begin{cases}k_{inc}\eta(t), E(t+1)<E(t)\\ k_{dec}\eta(t), E(t+1)>E(t)\\ \eta(t), \quad E(t+1)=E(t)\end{cases}$$

其中，t为训练次数，k_{inc},k_{dec}分别为递增乘因子和递减乘因子，$k_{inc}>1, 0<k_{dec}<1$。

(3)共轭梯度法

最速下降法是按照梯度下降最陡方向修正权值的。当梯度下降过快时会造成网络振荡，而下降过慢会降低网络的收敛速度。共轭梯度法是最速下降法的一种改进方法，用于解决各种最优化问题。共轭梯度法的搜索方向是在负梯度方向的基础上加上前一次搜索方向的共轭方向。

$S(t)$是网络所有权值分量组成的向量，$\eta(t)$是在$S(t)$方向上使误差达到极小的步长，$d(t)$是第t次搜索时的迭代搜索方向，第一次搜索时的方向是负梯度方向：

$$S(0) = -d(0) \tag{4-16}$$

利用共轭方向作为新一轮搜索方向并增加上一次搜索方向进行迭代，得到：

$$S(t) = -d(t) + \eta(t)S(t-1) \tag{4-17}$$

根据 $\eta(t)$ 的不同，可构成各种不同的共轭梯度法，最常见的有 Fletcher-Reeves 和 Polak-Ribiere 修正法，它们的修正式分别是：

$$\eta(t) = \frac{d(t)^T d(t)}{d(t-1)^T d(t-1)} \tag{4-18}$$

$$\eta(t) = \frac{\Delta d(t-1)^T d(t)}{d(t-1)^T d(t-1)} \tag{4-19}$$

(4)拟牛顿算法

一般的牛顿法中，搜索的迭代方程为：

$$S(t) = S(t) - A_t^{-1} d(t) \tag{4-20}$$

A_t^{-1} 是表现函数的二次导数，称为 Hessian 阵。

因为对于一般的神经网络，Hessian 阵计算量大。拟牛顿法就是通过引进一组矩阵来替代 Hessian 阵。拟牛顿法是求解非线性优化问题最有效的方法之一，拟牛顿法通过计算梯度的变化，构造一个目标函数的模型使之足以产生超线性收敛性。拟牛顿法的特点是不需要二阶导数的信息，又能很好的实现逼近。根据对 Hessian 阵修改方法的不同，拟牛顿法分为 DFP 法、BFGS 法等。

(5)LM(Levenberg-Marquardt)算法

LM 算法来源于牛顿法和梯度下降算法。LM 算法不仅利用了。目标函数的一阶信息，还利用了目标函数的二阶导数的信息。LM 算法通过雅克比(Jacobian)矩阵 J 来替代 Hessian 阵：

$$H = J^T J \tag{4-21}$$

其梯度为：

$$g = J^T e \tag{4-22}$$

其中，雅克比矩阵 J 是网络权值的函数。e 是网络误差向量。得到：

$$S(t+1) = S(t) - [J^T J + \lambda I]^{-1} J^T e \tag{4-23}$$

起初，λ 取一个很大的值，此时式(3-24)相当于梯度下降法；随着慢慢接近最优点，λ 减小到零，式(3-24)变成牛顿法。在训练过程中，如果误差性能良好，则减小 λ 的

值，否则增加λ的值，这样迭代下去直到找到最优点为止。

4.5.2.2 BP 网络的设计

选取 KDD99 数据集中具有 41 个特征的数据，经过数据预处理和 PCA 特征提取，送入 BP 网络。网络分训练和检测两个阶段。在训练阶段，一次训练将所有样本数据正向运行一轮并根据误差反向修改权值一次，这样反复训练，直到网络总误差达到精度要求或最大训练次数为止。在检测阶段，BP 网络对输入数据进行非线性映射，根据网络输出的不同判断是否发生入侵行为。

(1)网络的初始化

输入层神经元的个数取决于输入向量的位数，如果是经过了 PCA 特征处理过后的数据，输入层神经元的数目和处理后的数据维数相同。输出层神经元的个数取决于分类后类别的种类。网络的初始权值对网络的训练时间影响很大，一般选值在零点附近且足够小，本设计的所有权值都为-1～1 间随机数，设定最大收敛步长为 2000 步。

(2)隐层的设计

隐层的设计包括隐层数的设计和隐层节点数的设计。BP 神经网络可以有一个或多个隐层。单隐层的网络可以模拟所有的连续函数，多隐层网络可以模拟不连续的函数。在设计网络时，一般先采用单隐层的方法，如果网络的性能不佳，再考虑使用多隐层的神经网络。本设计的 BP 神经网络用的是单隐层网络。

隐层节点的作用是从样本中获取信息规律并存储起来，隐层与输入层、输出层都是通过权值连接起来，这些权值不断进行调整，以增强网络的映射能力。如果隐层节点个数过少，网络的映射能力就不强，起不到分类判别作用。若隐层节点个数过多，会降低网络的泛化能力，网络容易受噪声干扰，且会增加训练时间和检测时间。以下是计算隐层节点个数常用的公式：

$$n=\sqrt{n_i+n_o}+\alpha \tag{4-24}$$

$$n=\log_2 n_i \tag{4-25}$$

$$n=\sqrt{n_i\times n_o}+\alpha \tag{4-26}$$

其中，n_i, n_o分别是输入层的节点数和输出节点数，α取 1～10 之间的整数。本设计采用第一种计算方法。

(3)网络算法的改进

由于BP算法存在一些不足，所以在本设计中使用了多种BP网络的改进算法，有附加动量法、自适应学习速率法、共轭梯度法、拟牛顿算法和LM算法。

4.6 系统响应模块

入侵检测系统的响应模式[12]主要有主动响应和被动响应两种类型。被动响应是指入侵检测系统对检测到的入侵攻击采取简单地记录和报告的措施。主动响应是指入侵检测系统在检测到攻击后，能对入侵行为进行阻止和反击，并且能修正系统环境。本设计采用主动响应和被动响应相结合的模式。对于一些未知的或危害程度很低的入侵，只需要作出报告，记录日志或发出报警。对于一些已知确定的有一定危害性的入侵，不仅要记录日志和发出报警，而且要对入侵者进行反击，收集额外信息。对入侵者的反击方法有追踪入侵者的攻击来源，切断与攻击者的网络连接，过滤来自入侵者IP地址的数据包等。收集额外的信息是指用一些特别的服务器创造出一个假象使入侵者的入侵行为转向而入侵者却浑然不知，以此在保证系统网络安全的情况下记录入侵者的入侵行为。

第5章 实验及结果分析

5.1 实验数据及实验环境

本章所用的实验的硬件环境是 Intel Pentiun 双核 T4200 处理器，2G 主频，2G 内存，软件环境为 Microsoft Windows XP Home。实验所用的仿真软件是 Matlab R2009a 版本。

实验数据用的是 KDD99 数据集，该数据集在第四章已经介绍过。在数据集 corrected 和数据集 kddcup.data_10_percent_corrected 中，先按照 4.3 节的方法进行数据预处理，选取具有代表性的 neptune 攻击、back 攻击、ipsweep 攻击和 warezclient 攻击四种攻击各 800 条作分别与 2200 条正常数据记录构成训练样本。选取四种攻击数据记录各 200 条与 1000 条正常数据记录构成测试样本。

5.2 Kohonen 神经网络实验结果分析

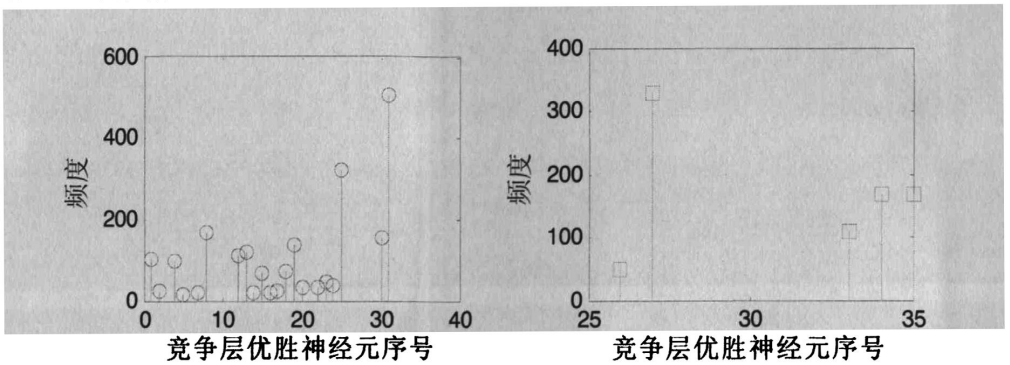
5.2.1 neptune 攻击的实验结果分析

1. 未经 PCA 处理的分析

把训练数据不经 PCA 特征提取直接送入 Kohonen 神经网络训练，训练后的神经元获胜频度如图 5-1 所示，横坐标是优胜神经元的序号，纵坐标表示在训练过程中该神经元序号成为优胜神经元的次数。(a)图为正常数据记录的优胜神经元的序号的获胜频度，(b)图为入侵攻击数据记录的优胜神经元的获胜频度。竞争层优胜节点的分布可以直观的用图 5-2 表示。“①”代表正常数据的优胜节点，“②”代表 neptune 攻击的优胜节点，空白表示不属于任何类别。节点序号的 1～2、4～5、7～8、12～24、30～31 属于正常数据优胜节点，序号 26～27、33～35 属于入侵攻击的优胜节点，可以看出，同类数据的优胜节点保持了位置上的相邻性，正常数据的优胜节点聚成一片大的区域，neptune 攻击的优胜节点形成了另一片聚集区。

训练好的神经网络的检测分类效果如图 5-3 所示。检测样本的前 1000 个为正常数据记录，后 200 个为 neptune 攻击数据记录。当测试样本对应的优胜节点与其类别

对应的优胜节点不符时，就认定神经网络分类错误。判断正确的情况用“*”表示，把正常的数据判断成neptune攻击的数据或者把neptune攻击的数据判断成正常的数据的情况用“○”表示。从图中可以看出，Kohonen网络出现了错误分类的情形，有一些正常数据样本被错认为是neptune攻击数据，有一小部分neptune攻击数据被当作了正常数据。



(a) (b)

图 5-1 Kohonen 网络训练后神经元频度分布

图 5-2 优胜节点分布

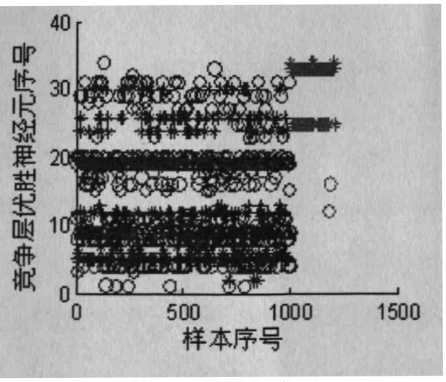


图 5-3 检测分类图

对网络的检测率、误报率、训练时间和检测时间进行统计，得到的结果如表5-1所示，表中数据都是平均值。从表中可以看出，Kohonen网络在未经过PCA特征提取的情形下，对neptune攻击的检测率很高，误报率较低。图5-4是统计检测率和误报率形成的ROC曲线。

表 5-1 训练和检测实验结果

平均检测率(%)	平均误报率(%)	训练时间(ms/样本)	检测时间(ms/样本)
97.2	2.6	0.808	0.143

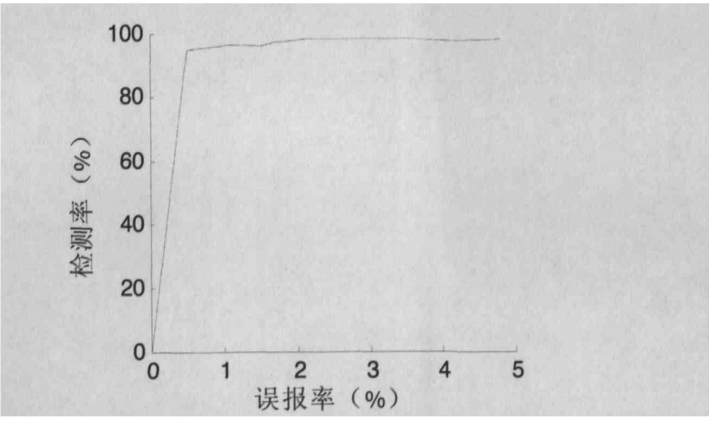


图 5-4　ROC 曲线图

2.经过 PCA 处理的分析

将实验样本经过主 PCA 特征提取，其中较大的 18 个特征值如表 5-2 所示。经计算，只要取前面 13 个特征值，其贡献率就可以达到 90%上。因此就可以把训练样本经过 PCA 算法后取前面较大的 13 个特征值对用的特征向量构成新的训练样本，这样就把样本数据的 41 维降成了 13 维。

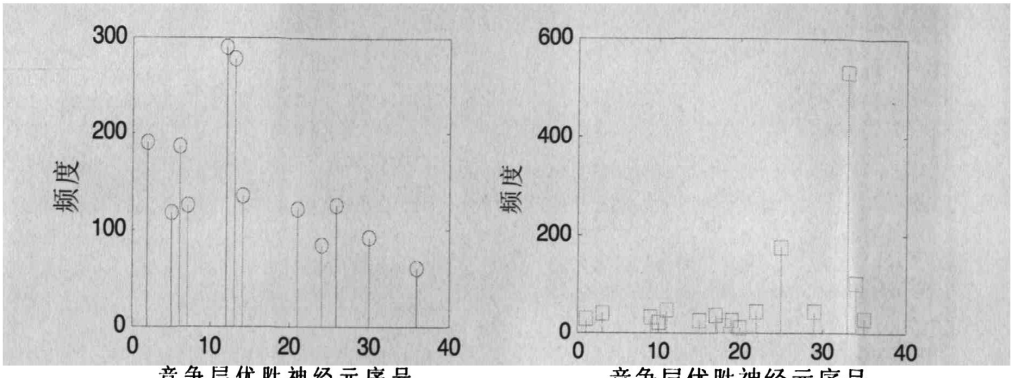
表 5-2 PCA 处理后的前 18 个特征值

特征项	1	2	3	4	5	6	7	8	9
特征值	8.1479	4.9974	3.2434	1.8857	1.5686	1.2081	1.1466	1.0935	1.0182
特征项	10	11	12	13	14	15	16	17	18
特征值	1.0030	0.9668	0.8667	0.8236	0.8032	0.7513	0.5656	0.4964	0.3638

把特征提取后的训练数据送入 Kohonen 神经网络训练，训练后的神经元获胜频度如图 5-1 所示。(a)图为正常数据记录的优胜神经元的序号的获胜频度，(b)图为入侵攻击数据记录的优胜神经元的获胜频度。竞争层优胜节点的分布可以直观的用图 5-2 表示。“①”代表正常数据的优胜节点，“②”代表 neptune 攻击的优胜节点，空白表示不属于任何类别。节点序号的 4～7、12～14、26、30、31、36 属于正常数据优胜节点，序号 9～11、17～21、33～35、1、3、15 属于 neptune 攻击优胜节点，可以看出，同类数据的优胜节点虽然在局部保持了一定的位置相关性，但总体来说比较分散，没有成片的相邻。

训练好的神经网络的检测分类效果如图 5-3 所示。检测样本的前 1000 个为正常数据记录，后 200 个为 neptune 攻击数据记录。判断正确的情况用“*”表示，把正

常的数据判断成neptune攻击的数据或者把neptune攻击的数据判断成正常数据的情况用“○”表示。从图中可以看出，正确样本的数据被误判为neptune攻击样本的情况是比较多的。



(a)　　(b)

图 5-5 Kohonen 网络训练后神经元频度分布

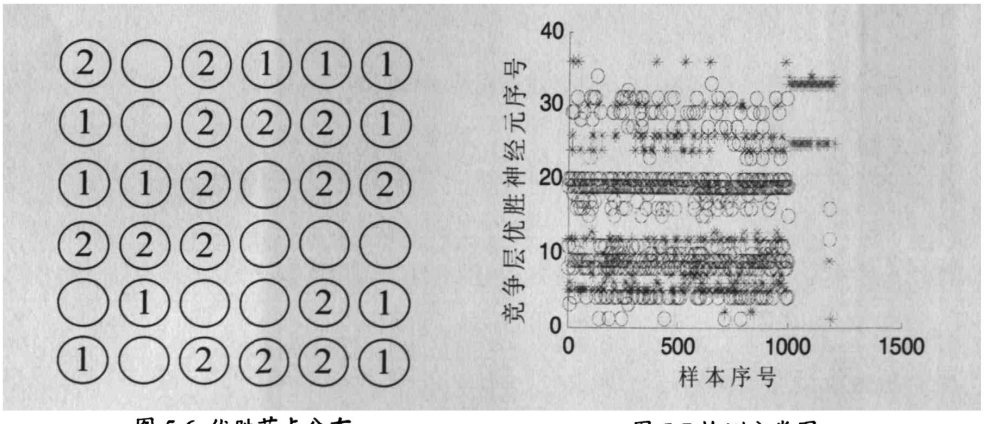


图 5-6 优胜节点分布　　图 5-7 检测分类图

对网络的检测率、误报率、训练时间和检测时间进行统计，得到的结果如表5-3所示，表中数据都是平均值。从表中可以看出，经过PCA处理后，Kohonen网络的训练时间没有明显变化，检测时间缩短了，检测率仍然处在一个较高的水平，但是误报率变得非常高。图5-4是统计检测率和误报率形成的ROC曲线。

表 5-3 训练和检测实验结果

平均检测率(%)	平均误报率(%)	训练时间（ms/样本）	检测时间（ms/样本）
97.6	30.7	0.803	0.119

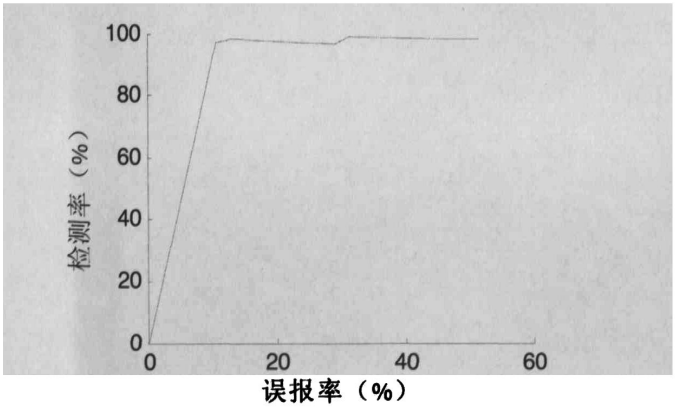


图 5-8 ROC 曲线图

总结：不管经过特征提取与否，Kohonen 神经网络对 neptune 都有很好的检测率，PCA 特征提取能够缩短网络的检测时间，这是由于特征提取在保留原数据绝大部分信息的情况下降低数据的维数，但是也付出了高误报率的代价，平均误报率达到 30.7%。如此高误报率的入侵检测系统在现实生活中是很难令人接受的，因此 PCA 特征提取不适宜用在对 neptune 攻击进行检测的系统中。

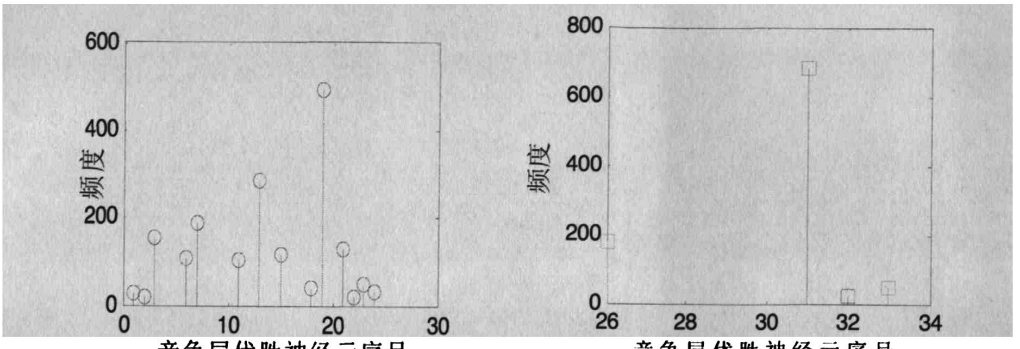
5.2.2 back 攻击的实验结果分析

1. 未经 PCA 处理的分析

实验步骤与上面 neptune 攻击检测实验基本相似，训练后的神经元获胜频度如图 5-9 所示，(a)图为正常数据记录的优胜神经元的序号的获胜频度，(b)图为入侵攻击数据记录的优胜神经元的获胜频度。竞争层优胜节点的分布可以直观的用图 5-10 表示。“①”代表正常数据的优胜节点，“②”代表 back 攻击的优胜节点，空白表示不属于任何类别。节点序号的 1～3、6～7、18～19、21～24、11、13、15 属于正常数据优胜节点，序号 31～33、26 属于 back 攻击优胜节点，可以看出，正常数据的优胜节点和 back 攻击数据的优胜节点的有着不同的分布，正常数据的优胜节点分布在前 24 个节点中，back 攻击数据的优胜节点分布在后面 12 个节点中。

训练好的神经网络的检测分类效果如图 5-11 所示。检测样本的前 1000 个为正常数据记录，后 200 个为 back 攻击数据记录。当测试样本对应的优胜节点与其类别对应的优胜节点不符时，就认定神经网络分类错误。判断正确的情况用“*”表示，把正常的数据判断成back攻击的数据或者把back攻击的数据判断成正常的数据的情况

用“○”表示。从图中可以看出，Kohonen 网络出现了错误分类的情形，有一些正常数据样本被错认为是 back 攻击数据，有一小部分入侵数据被当作了正常数据。



(a)　　(b)

图 5-9 Kohonen 网络训练后神经元频度分布

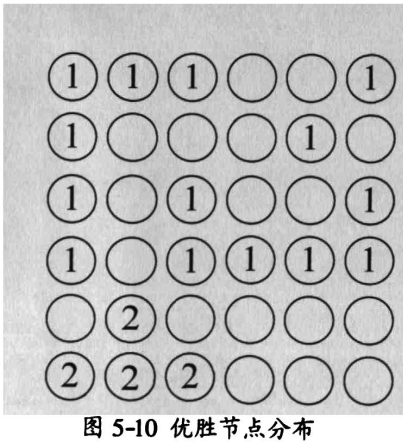


图 5-10 优胜节点分布

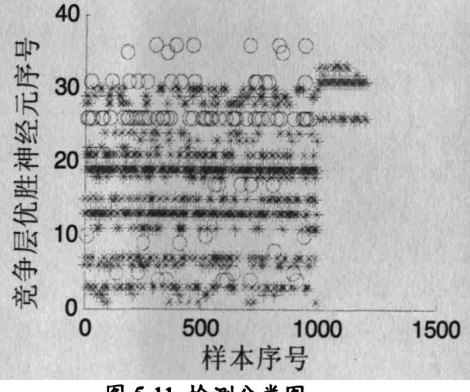


图 5-11 检测分类图

对网络的检测率、误报率、训练时间和检测时间进行统计，得到的结果如表 5-4 所示，表中数据都是平均值。从表中可以看出，Kohonen 网络在未经过 PCA 特征提取的情形下，对 back 攻击的检测率极高，误报率略为高了一些。图 5-12 是统计检测率和误报率形成的 ROC 曲线。

表 5-4 训练和检测实验结果

平均检测率(%)	平均误报率(%)	训练时间（ms/样本）	检测时间（ms/样本）
97.9	6.4	0.855	0.155

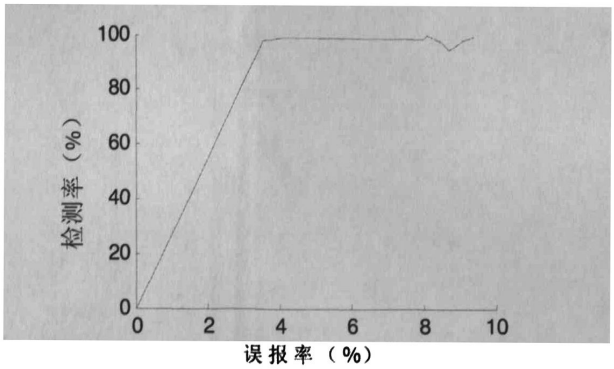


图 5-12　ROC 曲线

2. 经过 PCA 处理的分析

将实验样本经过主 PCA 特征提取，其中较大的 18 个特征值如表 5-5 所示。经计算，只要取前面 15 个特征值，其贡献率就可以达到 90%上。因此就可以把训练样本经过 PCA 算法后取前面较大的 15 个特征值对用的特征向量构成新的训练样本，这样就把样本数据的 41 维降成了 15 维。

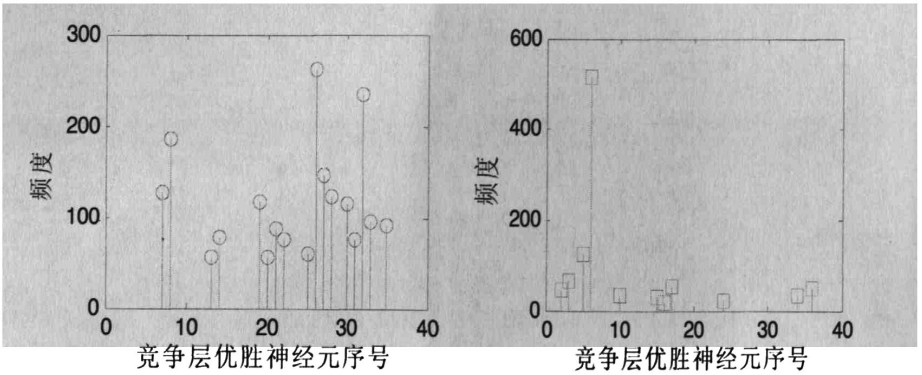
表 5-5 PCA 处理后的前 18 个特征值

特征项	1	2	3	4	5	6	7	8	9
特征值	8.3663	5.2136	2.9718	1.8673	1.7650	1.4066	1.1368	1.0206	1.0086
特征项	10	11	12	13	14	15	16	17	18
特征值	0.9803	0.9131	0.8639	0.7692	0.6367	0.5580	0.4411	0.3441	0.2237

把特征提取后的训练数据送入 Kohonen 神经网络训练，训练后的神经元获胜频度如图 5-13 所示。(a)图为正常数据记录的优胜神经元的序号的获胜频度，(b)图为入侵攻击数据记录的优胜神经元的获胜频度。竞争层优胜节点的分布可以直观的用图 5-14 表示。“①”代表正常数据的优胜节点，“②”代表 back 攻击的优胜节点，空白表示不属于任何类别。节点序号的 7～8、13～14、19～22、25～28、31～33、35 属于正常数据优胜节点，序号 2～3、5～6、15～17、24、34、36 属于 back 攻击优胜节点，可以看出，正常数据的优胜节点集中聚集在一片区域，back 攻击数据的优胜节点分布分散，没有形成大的聚集区。

训练好的神经网络的检测分类效果如图 5-15 所示。检测样本的前 1000 个为正常数据记录，后 200 个为 back 攻击数据记录。判断正确的情况用“*”表示，把正常的数据判断成back攻击的数据或者把back攻击的数据判断成正常的数据的情况用“○”

表示。从图中可以看出，Kohonen 神经网络出现了许多错误分类的情况。



(a)　　(b)

图 5-13 Kohonen 网络训练后神经元频度分布

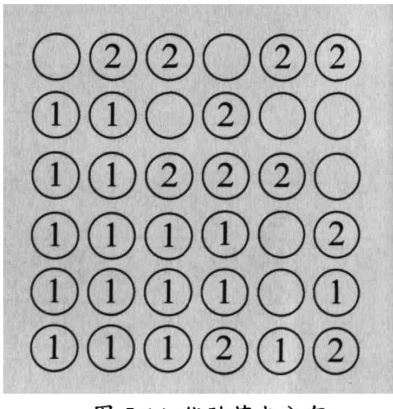


图 5-14 优胜节点分布

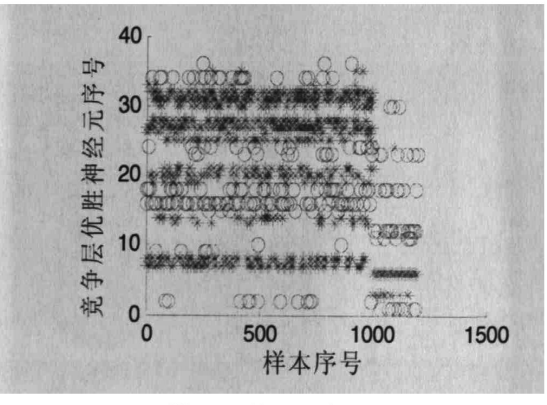


图 5-15 检测分类图

Kohonen 神经网络对 back 攻击的性能指标如表 5-6 所示。从表中可以看出，经过 PCA 处理后，Kohonen 网络的检测时间几乎没有变化，训练时间略微缩短了，平均误报率略高，但是检测率却很低。图 5-16 是统计检测率和误报率形成的 ROC 曲线。

表 5-6 训练和检测实验结果

平均检测率(%)	平均误报率(%)	训练时间（ms/样本）	检测时间（ms/样本）
69.5	8.6	0.818	0.154

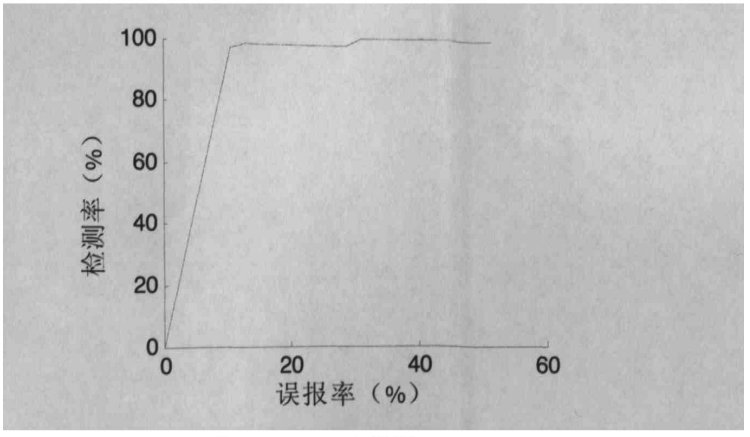


图 5-16 ROC 曲线图

总结：虽然经过 PCA 特征提取后 Kohonen 神经网络的训练时间略微缩短，但是检测率比未经特征提取下降了 28.4 个百分点，误报率也有所提高，网络的性能下降了很多。因此用在使用 Kohonen 神经网络检测 back 攻击时不建议用 PCA 特征提取方法。

5.2.3 ipsweep 和 warezclient 攻击的实验结果分析

按照上面实验的步骤，用 Kohonen 神经网络分别对 ipsweep 和 warezclient 攻击进行检测，实验结果如表 5-7 所示，表中数据都是统计后的平均值。

表 5-7 训练和检测实验结果

算法	检测率 (%)	误报率 (%)	训练时间 (ms/样本)	检测时间 (ms/样本)
PCA(ipsweep)	56.4	38.9	0.828	0.154
未经 PCA(ipsweep)	97.8	8.6	0.845	0.152
PCA(warezclient)	77.4	23.5	0.826	0.158
未经 PCA(warezclient)	96.2	6.4	0.859	0.153

从表中可以看出，无论是 ipsweep 攻击还是 warezclient 攻击，数据经过 PCA 特征提取后用 Kohonen 网络检测的效果都不佳，检测率很低，误报率很高，训练时间和检测时间也没有很明显的提高。不过，未经 PCA 特征提取的数据通过 Kohonen 网络检测的效果比较好，检测率很高，平均检测率达到 95%以上，误报率较好，其平均值介于 5%～10%之间。

5.3 BP 神经网络实验结果分析

5.3.1 neptune 攻击的实验结果分析

1. 未经 PCA 处理的分析

BP 神经网络的设计在 4.5.2 节已经介绍。输入层节点数取 41，输出层节点数取 1，隐层节点数按式(4-24)计算。将实验样本送入神经网络训练和检测，同时对 BP 算法进行改进。传统的 BP 算法是基于梯度下降法的，改进的算法有附加动量法、自适应学习速率法、Fletcher-Reeves 共轭梯度法（以下简称 FR 共轭梯度法）、Polak-Ribiere 共轭梯度法（以下简称 PR 共轭梯度法）、拟牛顿算法和 LM 算法。训练和检测结果如表 5-8 所示，表中所有的数据都是统计后的平均值。

表 5-8 训练和检测实验结果

算法	检测率 (%)	误报率 (%)	训练时间 (ms/样本)	检测时间 (ms/样本)
梯度下降法	95.8	3.6	2.511	0.0325
附加动量法	94.3	2.1	1.295	0.0283
自适应学习速率法	96.6	1.5	0.593	0.0299
FR 共轭梯度法	97.5	1.9	0.162	0.0287
PR 共轭梯度法	97.8	0.8	0.166	0.0293
拟牛顿算法	94.5	1.3	1.167	0.0292
LM 算法	97.1	0.6	1.064	0.0285

从表中可以看出，对于 neptune 攻击，传统的 BP 算法即梯度下降法训练时间和检测时间较其它改进后的算法来说较长，且误报率也比改进算法要高。改进后的六种 BP 算法在训练时间和检测时间上有不同程度的缩短，且误报率都降低了，检测率基本也很高。其中，两种共轭梯度法相对于其它改进算法而言在减小训练时间和检测时间方面最为成功，训练时间比传统 BP 算法缩短了约 14 倍，检测率有所提高，误报率也下降了。图 5-17 是梯度下降法和 FR 共轭梯度法的 ROC 曲线图，“*”形成的曲线是梯度下降法的 ROC 曲线，“□”形成的曲线是 FR 共轭梯度法的 ROC 曲线。FR 共轭梯度法的曲线更靠近坐标的左上方，因此 FR 共轭梯度法对 neptune 攻击的检测效果要好于梯度下降法。

传统的 BP 算法的网络训练误差曲线如图 5-18 所示。FR 共轭梯度法的网络训练误差曲线和 PR 共轭梯度法的训练误差曲线分别如图 5-19(a)和 5-19(b)所示。图的横坐标表示收敛步数。从图 5-18 和图 5-19 可以看出，在训练时，传统 BP 算法收敛步数很大，收敛缓慢，而用两种共轭梯度法改进的 BP 算法的收敛明显变快，这也证明了改进的 BP 算法能缩短网络的训练时间。

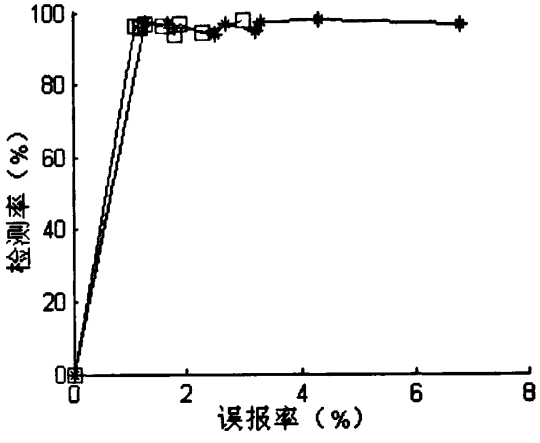


图 5-17 ROC 曲线图

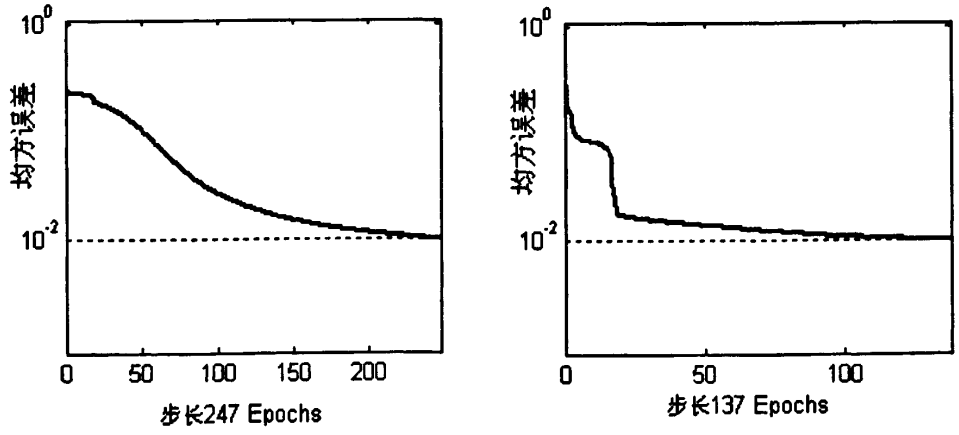


图 5-18 传统 BP 算法误差曲线图

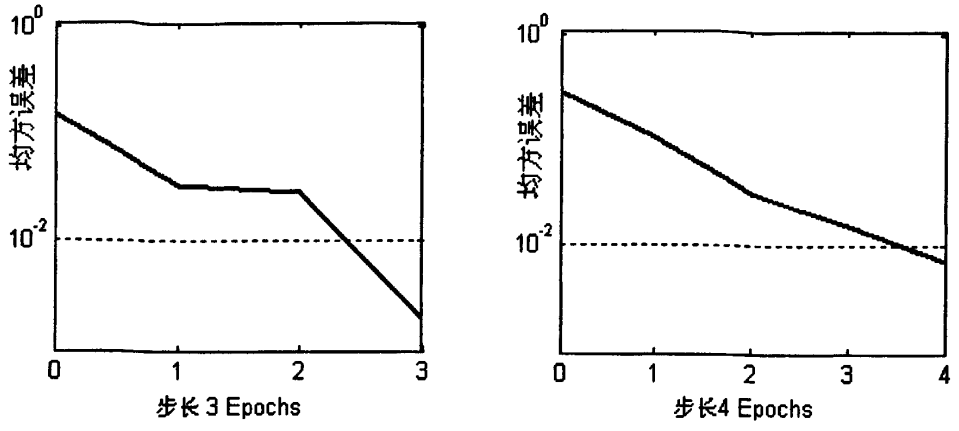


图 5-19 基于共轭梯度法的 BP 算法误差曲线图

2. 经过 PCA 处理的分析

将 PCA 特征提取后的数据送入 BP 神经网络进行训练和检测，实验结果如表 5-9 所示。对比表 5-8 和 5-9 可以看出，对于 neptune 攻击，样本在经过特征提取后的训练时间和检测时间都普遍缩短了，其中两个共轭梯度法的训练和检测时间最短，但 PR 共轭梯度法的误报率较高。除基于 LM 的算法外，其它改进算法的检测率与未经特征提取的相比变化不大，都很高，误报率整体都变高了，集中在 4%～7%之间。

表 5-9 训练和检测实验结果

算法	检测率 (%)	误报率 (%)	训练时间 (ms/样本)	检测时间 (ms/样本)
梯度下降法	97.4	6.6	0.614	0.261
附加动量法	96.1	6.8	0.519	0.249
自适应学习速率法	96.4	5.8	0.295	0.0267
FR 共轭梯度法	97.2	4.6	0.147	0.0245
PR 共轭梯度法	97.1	6.5	0.145	0.0248
拟牛顿算法	95.7	5.1	0.188	0.0250
LM 算法	91.2	5.6	0.251	0.0252

总结：从上述两个实验可以看出，对于 neptune 攻击，运用 PCA 特征提取技术和改进的 BP 算法，可以减小神经网络的训练时间和检测时间。但是使用 PCA 特征提取技术会增加入侵检测系统的误报率。对于用来检测 neptune 攻击的入侵检测系统来说，如果强调系统低误报率，而对系统的网络训练和检测实时行要求不高，不带 PCA

特征提取技术的基于共轭梯度改进算法的 BP 神经网络系统是个很好的选择。反之，可以选用带 PCA 特征提取的 FR 共轭梯度改进算法的 BP 神经网络的系统。

5.3.2 back 攻击的实验结果分析

1. 未经 PCA 处理的分析

实验按照与 neptune 攻击相同的实验步骤进行仿真。试验中发现，梯度下降法、附加动量法、自适应学习速率法、FR 共轭梯度法、PR 共轭梯度法和拟牛顿算法都出现了训练未收敛的情形(训练步长达到 2000 步时网络误差仍大于设定的最小误差)，如图 5-20 所示。只有基于 LM 算法的 BP 神经网络没有出现未收敛的情况。LM 改进算法的网络实验结果如表 5-10 所示。图 5-21 是其训练误差曲线图，在第 10 步的时候网络收敛。

表 5-10 训练和检测实验结果

算法	检测率(%)	误报率(%)	训练时间（ms/样本）	检测时间（ms/样本）
LM 算法	93.5	2.8	1.282	0.0130

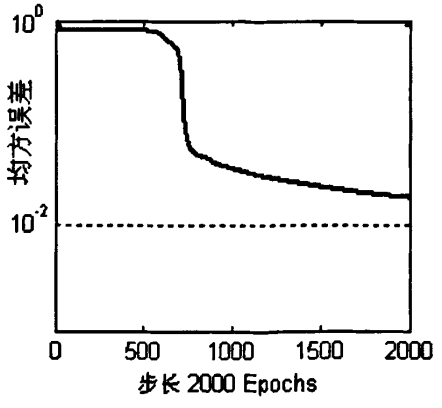


图 5-19　未收敛误差曲线图

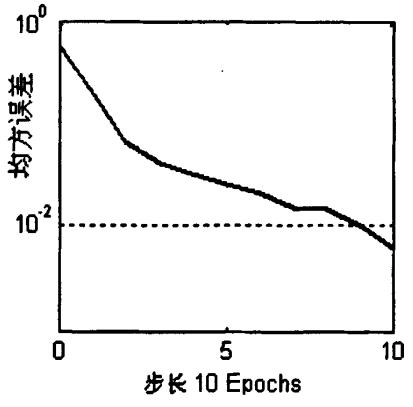


图 5-20　LM 算法误差曲线图

2. 经过 PCA 处理的分析

训练和检测的实验结果如表 5-11 所示。对于 back 攻击，FR 共轭梯度法、PR 共轭梯度法 、拟牛顿算法和 LM 算法的训练时间和检测时间比未经特征提取时减小了不少。FR 共轭梯度法和拟牛顿算法的训练误差曲线如图 5-21(a)和 5-21(b)所示，可以看出，这两个改进算法的收敛步长都很小。在改进算法中，FR 共轭梯度法的训练时

间最短，检测时间与最低的也相差无几。但是误报率各改进的算法方面普遍要比未经过 PCA 特征提取的 LM 改进算法要高 2～3 个百分点。

表 5-11 训练和检测实验结果

算法	检测率 (%)	误报率 (%)	训练时间 (ms/样本)	检测时间 (ms/样本)
梯度下降法	96.0	4.5	2.554	0.00995
附加动量法	96.5	4.6	2.368	0.0110
自适应学习速率法	96.3	4.1	4.982	0.0106
FR 共轭梯度法	95.7	4.8	0.163	0.00983
PR 共轭梯度法	95.9	3.9	0.331	0.00968
拟牛顿算法	96.4	5.1	0.431	0.00932
LM 算法	94.1	5.6	0.626	0.00971

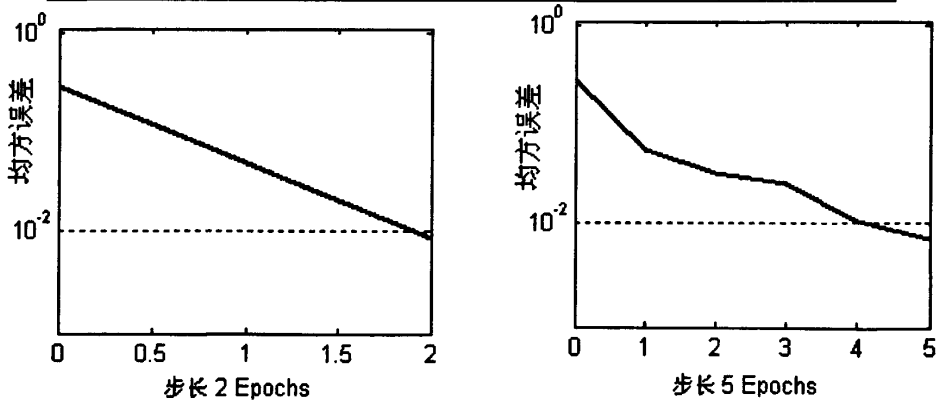


图 5-21 改进 BP 算法的训练误差曲线图

总结：从上述两个实验可以看出，对于 back 攻击，在没有运用 PCA 特征提取技术的情况下，传统的和改进的 BP 算法都存在着训练未收敛或训练时间很长的现象。而运用 PCA 处理数据后，训练时间和检测时间都大大缩短，没有训练未收敛的情形出现，而检测率基本能在 95%左右，误报率在 4%～5%左右，其 ROC 曲线如图 5-22 所示。基于 FR 共轭梯度法的改进 BP 神经网络的综合效果检测最好，因此可以把它应用到检测 back 攻击的入侵检测系统中。

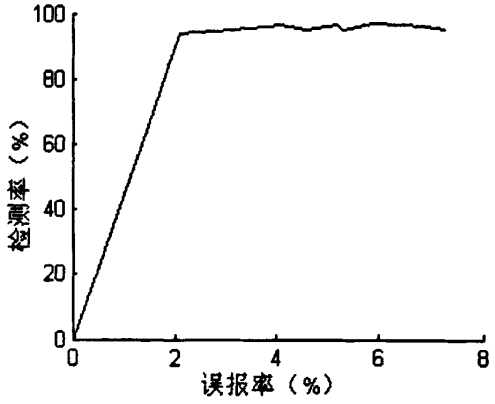


图 5-22 FR 共轭梯度法 ROC 曲线

5.3.3 warezclient 攻击的实验结果分析

1. 未经 PCA 处理的分析

实验按照与 neptune 攻击相同的实验步骤进行仿真。实验结果表明：梯度下降法、附加动量法和自适应学习速率法的 BP 网络在训练时无法收敛，无法收敛的误差曲线如图 5-23 的两幅图所示。

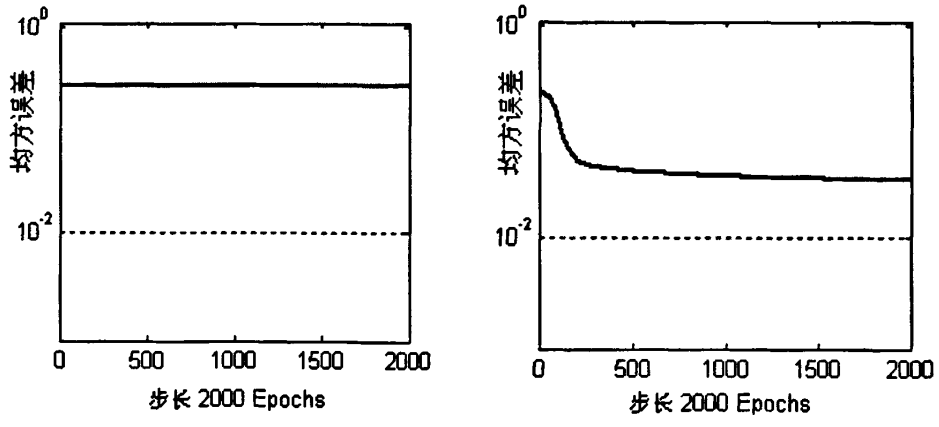


图 5-23 训练无法收敛的误差曲线图

训练和检测的实验结果如表 5-12 所示。从表中可以看出，在四种改进算法中，FR 共轭梯度法检测 warezclient 攻击的效果最好，其训练误差曲线和 ROC 曲线分别是图 5-24 和图 5-25。

表 5-12　训练和检测实验结果

算法	检测率 (%)	误报率 (%)	训练时间 (ms/样本)	检测时间 (ms/样本)
FR 共轭梯度法	95.8	3.1	0.219	0.130
PR 共轭梯度法	95.2	3.5	0.234	0.130
拟牛顿算法	94.4	3.9	0.657	0.131
LM 算法	96.5	3.6	0.682	0.133

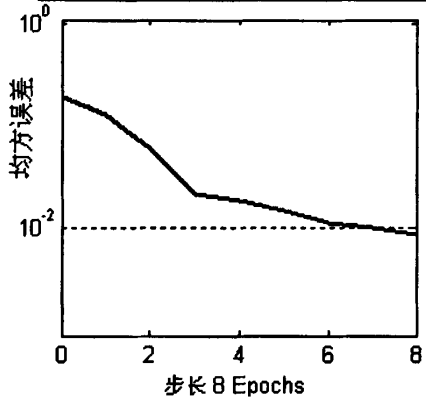


图 5-24　FR 共轭梯度法误差曲线

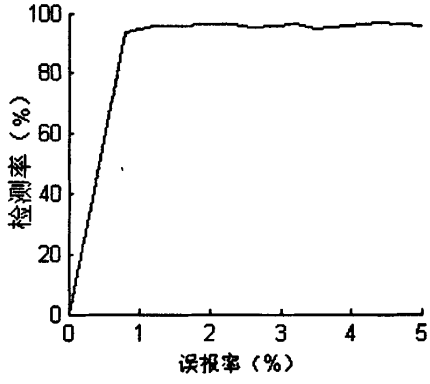


图 5-25　FR 共轭梯度法 ROC 曲线

2. 经过 PCA 处理的分析

实验结果如表 5-13 所示。梯度下降法和附加动量法相对于其它算法来说训练时间较长，而 PR 共轭梯度法、拟牛顿算法的训练时间很短。梯度下降法和拟牛顿算法的收敛曲线分别如图 5-26 和图 5-27 所示，可以看出，拟牛顿法的收敛步长比梯度下降法小的多。LM 算法的检测率较低。自适应学习速率法、附加动量法和拟牛顿算法的检测时间较低。

表 5-13　训练和检测实验结果

算法	检测率 (%)	误报率 (%)	训练时间 (ms/样本)	检测时间 (ms/样本)
梯度下降法	94.3	5.9	1.901	0.0108
附加动量法	95.1	6.4	1.763	0.00949
自适应学习速率法	94.9	6.4	0.432	0.00937
FR 共轭梯度法	95.2	5.2	0.163	0.01026
PR 共轭梯度法	93.8	6.6	0.162	0.0130
拟牛顿算法	96.5	3.8	0.431	0.00978
LM 算法	86.9	4.5	0.155	0.0116

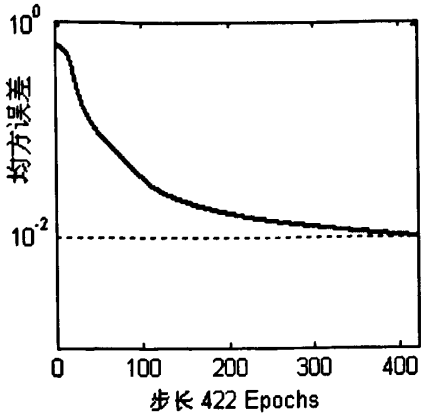


图 5-26 梯度下降法误差曲线

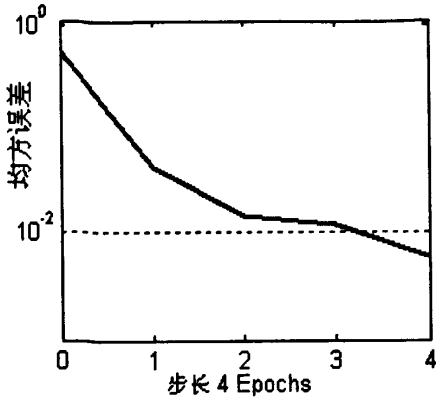


图 5-27 拟牛顿算法误差曲线

综合来看，拟牛顿算法的训练时间最短，仅为梯度下降法的 1/12，误报率最低，检测率最高，因此检测 warezclient 攻击的效果好，其 ROC 曲线如图 5-28 所示。

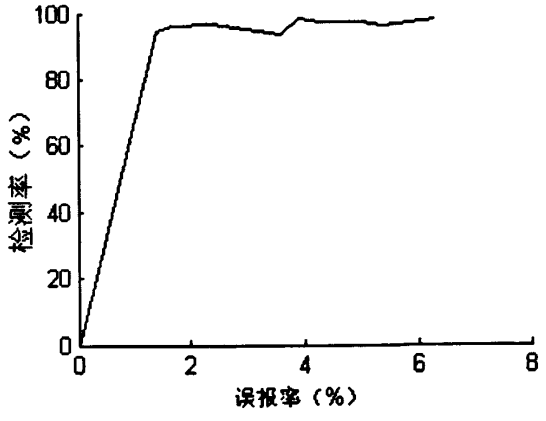


图 5-28 拟牛顿法 ROC 曲线

总结：未经 PCA 特征提取的 warezclient 攻击数据通过 BP 神经网络训练会出现未收敛的情形，而特征提取后没有这种现象。对比表 5-13 和表 5-12 发现，特征提取后通过拟牛顿算法的网络检测效果要比未特征提取的任何算法的网络要好。所以将基于拟牛顿算法的 BP 神经网络应用在入侵检测系统中，可以很好的检测 warezclient 攻击。

5.3.4 ipsweep 攻击的实验结果分析

1. 未经 PCA 处理的分析

按照与 neptune 攻击相同的实验步骤进行仿真。在实验中发现：没有用 PCA 特征提取处理数据时，梯度下降法、附加动量法、自适应学习速率法和拟牛顿算法在训练时出现无法收敛的情形。实验结果如表 5-14。

表 5-14 训练和检测实验结果

算法	检测率 (%)	误报率 (%)	训练时间 (ms/样本)	检测时间 (ms/样本)
FR 共轭梯度法	97.5	4.1	0.450	0.121
PR 共轭梯度法	96.1	4.8	0.459	0.133
LM 算法	96.0	3.2	0.822	0.141

2. 经过 PCA 处理的分析

实验结果如表 5-15 所示。七个算法在实验过程中没有出现训练未收敛的情况，其中，PR 共轭梯度法和拟牛顿算法的训练时间很短，比是梯度下降法和附加动量法缩短了十几倍。LM 算法的检测率较低，误报率较高。综合看，PR 共轭梯度法是最优的检测方法，它的训练误差曲线和 ROC 曲线如图 5-29 和图 5-30。

表 5-15 训练和检测实验结果

算法	检测率 (%)	误报率 (%)	训练时间 (ms/样本)	检测时间 (ms/样本)
梯度下降法	97.8	2.0	3.029	0.0124
附加动量法	94.9	2.2	2.911	0.0109
自适应学习速率法	96.1	2.3	0.496	0.00944
FR 共轭梯度法	96.6	4.7	0.330	0.0133
PR 共轭梯度法	95.4	4.5	0.244	0.0122
拟牛顿算法	95.9	5.3	0.431	0.0111
LM 算法	90.5	10.0	0.249	0.0129

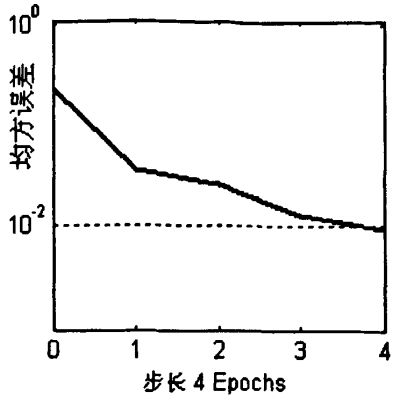


图 5-29 PR 共轭梯度法误差曲线

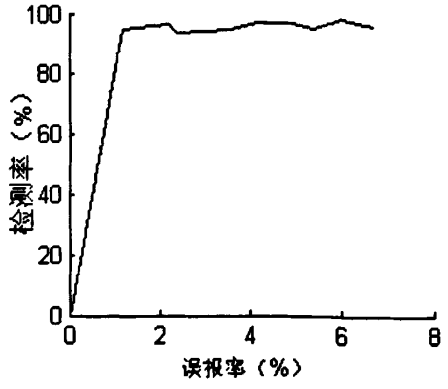


图 5-30 PR 共轭梯度法 ROC 曲线

总结：ipsweep 数据经过 PCA 特征处理后再送入神经网络，可以避免出现训练未收敛的情况，且训练时间和检测时间都缩短了。利用改进的 BP 算法，也能提高网络的实时性。基于 PR 共轭梯度法的改进 BP 神经网络可以很好的检测 ipsweep 攻击。

5.4 Kohonen 网络和 BP 网络的对比分析和总结

本设计分别将 Kohonen 网络和 BP 网络应用在入侵检测系统中，检测 neptune、back、warezclient 和 ipsweep 四种入侵攻击。Kohonen 网络在处理未经 PCA 特征提取的数据时，检测率较高，普遍 95%以上，误报率在 10%以内，误报率最低的是 neptune 攻击的检测，为 2.6%，误报率最高的是 ipweep 攻击的检测，为 8.6%。Kohonen 网络处理 PCA 特征提取后的数据都不理想，虽然 PCA 特征提取技术降低了数据的维数。从检测率看，只有对 neptune 攻击的达到 90%以上，其余攻击的均在 80%以下；从误报率看，除了对 back 攻击的小于 10%，其余几个攻击的都超过 20%；从训练时间和检测时间来看，减小的幅度在 10%之内，没有明显的效果。出现这种情况的原因可能是 PCA 特征提取技术可能在降低维数的同时破坏了样本数据间内在的某些联系，而 Kohonen 网络恰好是根据这些内在联系进行数据分类的。

本设计在研究 BP 神经网络的时候对传统的基于梯度下降法的 BP 算法进行了改进，一共用了 6 种改进算法。从实验结果看，PCA 特征提取技术和改进的 BP 算法两者均可以减小网络训练未收敛的几率，缩短训练时间和检测时间。在 6 种改进的 BP 算法中，两种共轭梯度法、拟牛顿算法和 LM 算法的效果比较显著，能较大的幅度地

降低训练和检测时间。把 PCA 特征提取技术和 BP 改进算法相结合，可以极大的缩短训练时间和检测时间，训练时间一般比原来缩短十几倍甚至几十倍，检测时间一般缩短 20%以上。Kohonen 神经网络的训练时间一般是 2～3 毫秒/样本，检测时间一般是 0.8～0.9 毫秒/样本，较优的改进 BP 神经网络的的训练时间可以减小到 0.1~0.3 毫秒/样本，检测时间可以减小到 0.009~0.013 毫秒/样本。与 Kohonen 神经网络相比，改进后的 BP 网络的训练时间和检测时间大大缩短了，而两者的检测率和误报率差别不大。因此，将数据经 PCA 特征提取后，再通过改进的 BP 神经网络进行检测能取得很好的识别效果。

第6章 结论与展望

6.1 结论

在当今，计算机安全成为全世界广泛关注的热点话题，计算机的应用已经深入到社会和生活的各个方面。入侵检测系统的兴起和发展就是为了保证计算机和网络的安全。随着互联网的日益普及和网络入侵攻击的日益增多，入侵检测系统起到的作用越来越大。本文将PCA特征提取技术和神经网络技术应用在入侵检测系统中，主要工作有以下几方面：

(1) 对入侵检测的概念作了阐述，介绍了不同类型的入侵检测系统的体系结构，如基于主机的入侵检测系统和基于网络的入侵检测系统，并分析各自的优缺点和适应的场合。综合总结了各种不同的入侵检测技术。详细描述了人工神经网络中的Kohonen网络和BP网络的算法和学习方式。

(2) 在综合多种入侵检测系统模型的基础上，根据模块化的思想设计出了一个新的入侵检测系统结构。将PCA特征提取技术应用到这个系统结构中，用以降低数据的维数。针对基于梯度下降法的BP神经网络的固有缺陷，提出了六种改进算法。

(3) 将设计好的入侵检测系统进行实验仿真。把训练时间、检测时间、检测率和误报率作为实验的评估指标，对比Kohonen神经网络和改进BP神经网络的实验结果，得出检测四种攻击类型的最佳算法。从实验结果中得出：将PCA特征技术和改进BP神经网络相结合，能很好的检测入侵攻击，且实时性良好。

6.2 展望

(1) 把神经网络应用到入侵检测系统中是一项新的研究，本文用到的人工神经网络技术是Kohonen和BP两种网络。人工神经网络还包括RBF神经网络、Hopfield神经网络等，在以后的工作中可以研究这些网络在入侵检测中的应用，综合分析各类型神经网络的优缺点，最大发挥各神经网络的检测效果。

(2) 本文只是研究了四种攻击类型的检测，但入侵攻击的手段种类繁多，且变化很快，所以本设计的入侵检测系统还没有做到对攻击的全面检测，还要继续对攻击种类的检测方面进行全面研究。

(3) 在对入侵检测系统的性能评价方面，是从检测率、误报率、训练时间和检测时间四个方面入手的。仅用这四个方面评价有时候是不够的。在设计入侵检测系统时，还应考虑到系统资源的占用情况、系统的负荷能力和检测范围、系统的响应方式和更新维护的难易程度等。这些内容都需要进一步去研究和完善。

参考文献

[1] 第 29 次中国互联网络发展状况统计报告[R]. 中国互联网络信息中心,2012.

[2] 胡建伟. 网络安全与保密[M]. 西安: 西安电子科技大学出版社, 2003:23~24.

[3] A. Wool. Architecting the Lumeta Firewall Analyzer. USENIX Security Symp, Aug.,2001,12:45-47.

[4] Smaha,S.E.,T.A.S.Inc. Austin.Haystack:An intrusion detection system.1988: 37-44.

[5] J.P.Anderson. Computer Security Thread Monitoring and Surveillance[J]. Technical Report Jame P.AndersonCo. ,Fort Washington, PA.APr.1980.1994, 5:28-42.

[6] Dorothy E.Denning. An Intrusion Deteetion Model[J]. IEEE TRANS On Software Engineering,14(2):120-137.

[7] Colin Campbell. An Introduction to Kernel Methods.Radial Basis Function Netwoks:Design and applications. 2000,2(1):45-56.

[8] Jaeob WUlvila, John E Gaflhey Jr. Evaluation of Intrusion Deteetion Systems. Joumal of Research of the National Institute of standards and Technology, 2011, 108(6):14 -15.

[9] 杨贸云. 信息与网络安全实用教程[M]. 北京: 电子工业出版社, 2010.

[10] 唐正军. 入侵检测技术导论[M]. 北京: 机械工业出版社,2004:38~39.

[11] 宁宇鹏, 薛静锋. 入侵检测技术[M]. 北京: 机械工业出版社,2004:96-101.

[12] 鲜永菊. 入侵检测[M]. 西安: 西安电子科技大学出版社, 2009:56-59.

[13] 曹元大, 薛静锋. 入侵检测技术[M]. 北京: 人民邮电出版社, 2007:141-145.

[14] T.Fawcett. ROC Graphs: Notes and Practical Considerations for Researchers. Technical report,Palo Alto,USA:HP Laboratories.2004:2-3.

[15] Eugene H.Spafford,Diego Zambon. Intrusion Detection Using Autonomous Agents[J] .Computer Network ,2007,15(34):221-248.

[16] SMAHA S E.Haystack. An Intrusion Detection System:proceedings of IEEE Fourth Aerospace Computer Security Applications Conference[C]. Orland,FL. 1988.

[17] 杨亿先,钮心忻. 入侵检测理论与技术[M]. 北京:高等教育出版社, 2006.

[18] B.Mukherjee,L.Thbeerlein,K.N.Lveitt. Network intursion detection. IEEE Network,1994: 26-30.

[19] R HEADY,G.LUGER,A MACCABE,M SERVILLA,The architecture of a network

level intrusion detection system,Technical report CS90-20,University of New Mexico[D],1990.

[20] 黄卢记. 基于网络行为分析的入侵检测系统研究[J]. 计算机研究与发展，2005,11(4):128-129.

[21] Cuppen F,Miege A. Alert correlation in a cooperative intrusion detection framwork:proceed-ings of 2002 IEEE Symposium on Security and Privacy[C]. Oakland,USA,2008.

[22] Anderson D，Frivold Th，valdes A.Next-generation Intrusion-Deteetion Expert System[J].A Summary,SRI-CSL-95-07，SRI Internation，Menlo Park,CA,1995(5):2-8.

[23] S.Kumar.Classifieation and Detection of Computer Intrusion[D]. USA:Dept.of Computer Scienee,Purdue University,1995.2.

[24] TA.Gilham，J.Jagannathan. A real time intrusion detection expert system[Z]. Technical Report. SRI International,Computer Science Lab，SRI-CSL-92-05，1992(05):5-12.

[25] PA.Porras.STAT :A State Transition Analysis Tool for Intrusion Detection[D]. M.S.Thesis,Computer Science Department,University of California Santa Barbara，1992(6).

[26] P.Helman,G.Liepins,W.Richards.Foundations of intrusion detection. Proc.15th Computer Security foundations Workshop Franconic. NH,June 1992:114-120.

[27] LEE W,SAL STOLFO. Data mining approached for intrusion detection: proceedings of the Seventh USENIX Security Symposium[C]. San Antonio,TX,2004.

[28] 蒋良孝. 朴素贝叶斯分类器及其改进算法研究[D]. 中国地质大学博士学位论文，2009 .

[29] 李继硕. 人工神经网络基础[M]. 北京：高等教育出版社，2002.

[30] A.Patcha,J.-M.Park. An overview of anomaly detection techniques-Existing solutions and latest technological trends. Computer Networks,2007,51:3448–3470.

[31] 罗光春.入侵检测系统的现状与研究进展[J].北京邮电大学学报,2009,8(10):24-25.

[32] Joo D.,Hong T.,Han I.. The Neural Network Models for IDS Based on the Asymmetric Costs of False Negative Errors and False Positive Errors[J]. Expert Systems with Applications, 2003,25(1):69-75.

[33] GELENBE E. Learining in the recurrent random neural network[J]. Neural

Coputation,2009,5(1):154-164.

[34] P.FRASCONI, M.GORI,G.Soda. Local feedback multilayered networks[J]. Neural Computer,1992(4):120-130.

[35] Hopfield J.J..Neural Networks and Physical Systems with Emergent Collective Computational Propertied[J]. Proceedings of the National Academy of Sciences, 1982,79:2554-2558.

[36] 焦李成. 神经网络系统理论[M]. 西安: 西安电子科学出版社,1995.

[37] 杨行俊，郑君里. 人工神经网络[M]. 北京: 高等教育出版社,1992.

[38] Kohonen T.Self-Organization and associative memory[C]. Berlin: Springer Verlag,1989.

[39] MarKay D.J.C..A Practical Bayesian Framework for Backprop Networks[J]. Neural Computation,2007,4:448-472.

[40] S.Axelsson. Intrusion detection systems:A survey and taxonomy[J]. Technical Report Department of Computer Engineering,Chalmers University.March 2008.

[41] McCanne S.Jacobson . The BSD Packet Filter:A New Architecture for User-level Pack Capture[C]. Proceedings of the 1993 Winter USENIX Technical Conference. USENIX,1993.

[42] Lee W,Stolfo SJ. A data mining framework for building intrusion detection model[J]. In:Proc. of the 1999 IEEE Symp. on Security and Privacy. Oakland,1999,23:120-132.

[43] MIT Lincoln Laboratory. http://www.ll.mit.edu/IST/ideval.

[44] Mollestad T,Skowron A. A Rough Set Framework for Data Mining of Propositional Default Rules[M]. Twelfth Intl Conf on Data Engineering.1996.

[45] Joel Scambray,Stuart McClure 著. 杨洪涛译. 网络黑客大曝光: 网络安全机密与解决方案[M]. 北京: 清华大学出版社，2002: 195-221.

[46] 齐敏，李大健. 模式识别导论[M]. 北京: 清华大学出版社，2009: 128-130.

[47] Ian T Jolliffe. Principal Component Analysis[M]. New York: Springer Verlag, 1986:150-153.

[48] 赵广社,张希仁. 基于主成分分析的支持向量机分类方法研究[J]. 计算机工程与应用,2004,3:37-39.

[49] HUNT K J,SBARBARO D,ZBIKOWSKI R.Neural Networks for Control System-A Survey[J].Automatica,2006,6(28):1083:1112.

[50] 周志华，曹存根. 神经网络及其应用[M]. 北京：清华大学出版社,2004.

[51] 张德丰.MATLAB 神经网络编程[M]. 北京：化学工业出版社，2011.

攻读硕士期间发表的论文

1. 陈熹，朱灿焰. 两种神经网络在入侵检测中的应用[J]. 通信技术，2011,44(11)：106-108.

致谢

三年的研究生生涯即将过去，回想起这三年的学习和生活，感慨颇多。一路走来，得到了很多人的帮助，这里我要表示衷心的感谢。

首先衷心感谢我的导师朱灿焰教授！从论文的选题到到论文的完成，朱老师给了我无私的帮助。朱老师都以严谨的治学态度及敏捷的思维使我受益匪浅。在论文的写作过程中，朱老师给了我很多建议，教了很多学习的方法，使我少走了许多弯路，培养了自己的独立思考的能力和文献的阅读水平。可以说，朱老师在这篇论文上也倾注了大量心血。朱老师的为人处事的态度和孜孜不倦的工作精神是我以后学习的目标和榜样。在此，特向朱老师表示最衷心的感谢！

其次，感谢同一实验室的赵超、卢慧英同学和师兄李睿、杨伟、钱兰君同学的无私帮助，感谢你们每次不厌其烦的言传身教，使我学到了很多。感谢同一宿舍的庞磊、许超同学，和你们的相处非常愉快，是你们开阔了我的眼界，在困难的时候不断鼓励我继续前进，希望他们在以后的工作中不断进步，生活幸福！

最后要感谢我的家人，感谢他们对我的支持，希望他们身体健康！