混合入侵检测系统的研究

高 峥，陈蜀宇，李国勇
（重庆大学 软件学院，重庆 400044）

摘 要：针对入侵检测系统中的误用检测和异常检测两种检测方法存在的不足，在研究混合型入侵检测系统的基础上，提出一种混合型入侵检测系统的设计方案。设计方案将两种检测方法混合，误用检测采用模式匹配算法；异常检测是利用自组织神经网络对数据进行聚类，然后通过有监督的学习矢量量化对初聚类的数据进行再分类，使异常检测模式库有更加清晰的规则集。最后对系统的关键模块进行了仿真实验。仿真实验结果表明，此设计方案提高了混合入侵检测系统的检测能力和检测的准确率。

关键词：入侵检测；误用检测；异常检测；神经网络
中图分类号：TP311 **文献标识码**：A **文章编号**：1673－629X(2010)06－0148－04

Research of a Hybrid Intrusion Detection System

GAO Zheng, CHEN Shu-yu, LI Guo-yong
(College of Software Engineering, Chongqing University, Chongqing 400044, China)

Abstract: Aiming at the shortages of misuse detection and anomaly detection in intrusion detection system, on basis of researching hybrid intrusion detection system, a new design of hybrid intrusion detection system was proposed by studying it. Misuse detection module is based on Snort's pattern rules database. Anomaly detection is to use self－organizing neural network for data clustering, and then to classify these data by supervised learning vector quantization. Simulation of the key modules in this system was done successfully, and results show that the system improved capabilities and accuracy of the hybrid intrusion detection system.

Key words: intrusion detection; misuse detection; anomaly detection; neural networks

0 引 言

入侵检测（Intrusion Detection，ID）通过对计算机网络或计算机系统的信息收集并进行分析，发现网络或者主机中是否有违反安全策略的行为和入侵攻击的迹象。入侵检测系统（Intrusion Detection System，IDS）是具有入侵检测功能的软件与硬件结合的一套系统。

随着网络上的攻击种类变得繁多，攻击频率逐渐加强，网络安全已逐渐受大家重视。IDS已成为网络安全不可缺少的一环，但现有的入侵防御系统大都采用单一的入侵检测方法，或采用滥用检测或采用异常检测，从而使入侵检测系统降低了深度检测的能力[1]。

根据入侵检测方法的不同，可以分为误用检测（misuse detection）和异常检测（anomaly detection）两种。误用检测是通过专家系统建立的规则库来匹配网络上的攻击行为，而异常检测是分析网络数据，区分出正常流量及非正常流量，从而检测出异常数据。但是，由于两种检测方式的局限性，导致两种检测方法都具有明显缺陷，误用检测虽然可以很好地检测已知攻击行为，但它是历史性的，不能够根据网络攻击的改变而做出变化，现在的网络中新型的攻击日益复杂，如若检测不出新型的网络攻击则不能保护宿主机或局域网络；异常检测技术很好地弥补了这个问题，它通过各类数据挖掘算法分析网络中的非正常数据，检测出异常的攻击，而异常检测往往需要相对较长的训练时间完成规则集，分析出攻击行为的特征，并且要求训练时的样本数据空间包含所有的网络攻击集，目前一直没有一个很好的解决方案能够使异常检测训练出完整的规则集。

笔者阅读大量文献发现[2~4]，无法找到一种算法，让异常检测具有良好的网络环境适应性，无需提前训练就能够应用到入侵检测中。因此文中从系统结构入手，结合两种入侵检测方法联合处理，解决现有入侵检

收稿日期：2009－10－11；**修回日期**：2010－01－13
基金项目：教育部新世纪优秀人才支持计划项目（NCET－04－0843）；重庆市信息产业发展基金项目（200611009）；重庆市自然科学基金资助项目（2005BB2192）
作者简介：高 峥（1983－），男，天津宝坻人，硕士研究生，研究方向为计算机网络安全；陈蜀宇，博士，教授，博士生导师，研究领域为计算机网络安全、可信计算、网络终端及嵌入式系统。

测系统问题。

1　混合入侵检测系统

1.1　系统介绍

下面是混合入侵防御系统的结构图,如图 1 所示。

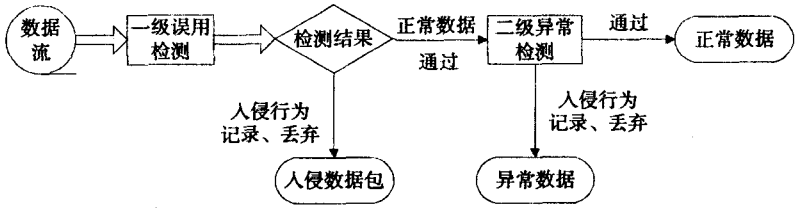

图 1　入侵防御系统结构图

混合入侵防御系统[5]首先通过误用检测,然后根据检测的结果,如果通过误用检测出是具有入侵行为的数据包,则记录攻击行为并丢弃网络数据包,如若是正常数据,则进入二级的异常检测。在异常检测模块中检测的是将已知的网络攻击过滤掉的网络数据,此时将网络数据备份,通过根据神经网络聚类算法提炼的规则集。备份的网络数据是用来为神经网络聚类提炼规则集的数据,这样处理大大提高了整个系统的检测效率。下面对各部分进行详细介绍。

1.2　误用检测模型

误用检测要求效率高,并且是可检测已知的所有攻击行为的模型,文中采用开源的 Snort 入侵检测作为误用检测模块。

Snort[6]作为一种开放源代码基于误用检测规则的系统已得到广泛的应用,它采用基于规则的网络信息搜索机制,通过对数据包内容进行模式匹配来检测多种不同入侵行为和探索活动。Snort 开源的入侵检测包主要包括包解码器、检测引擎、规则集主要部分。系统结构如图 2 所示。

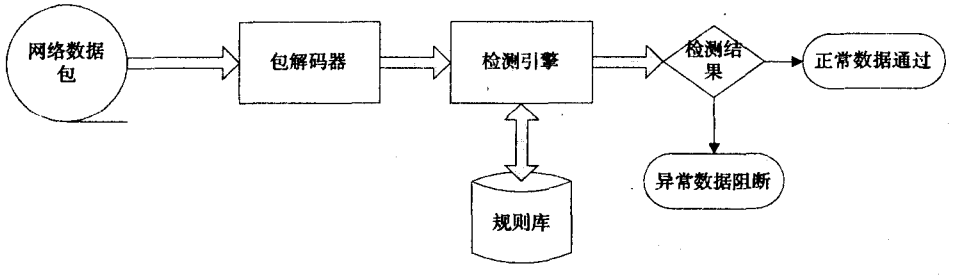

图 2　Snort 工作系统结构

首先,截获网络数据包,通过包解码器对各协议栈上的数据包进行解析和预处理,解析过程是考验整个入侵检测系统的检测速度和是否有丢包的重要依据,所完成的主要功能包括形成处理协议链表、解析 IP 地址、端口号和数据包负载等信息,然后将处理结果交给检测引擎;检测引擎按照规则库加载的规则,对数据包进行树形的模式匹配,探测数据包是否包含已知的入侵行为;如检测出异常数据,则报警日志模块,记录日志并丢弃数据包;如未检测出异常,则正常数据包进入系统下一个模块。

1.3　异常检测模型

1.3.1　自组织映射(SOM)神经网络

基于生物神经元之间"加强中心而抑制周围"的现象,1982 年芬兰学者 Kohonen 提出了自组织映射神经网络[7],SOM 神经网络属于竞争神经网络的一种,获胜神经元不但加强自身,而且带动周围邻近神经元得以相应的加强,同时抑制周围距离较远的神经元。

1.3.2　SOM 网络的结构

SOM 网络的拓扑结构如图 3 所示:从网络结构上看,自组织神经网络的最大特点是神经元被放置在二维的网络节点上。该模型包含输入输出两层,而不包含隐层。输入层中神经元个数由输入模式的特征数决定,一般是一个特征对应一个输入神经元,输出层的神经元个数的选取直接影响 SOM 网络的性能。输入模式的每个元素均连至输出层上的每个神经元。

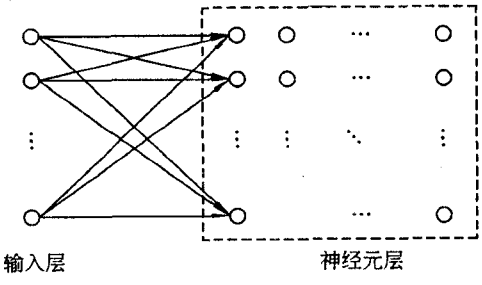

图 3　SOM 神经网络网络模型

1.3.3　SOM 学习算法

自组织映射[8]学习算法属于无监督竞争学习算法。能够对输入模式进行自动的聚类,即在无监督的情况下,通过输入模式的自组织学习,在输出层将聚类结果表示出来。与其他类型的神经网络的区别在于它不是以一个神经元的状态矢量反映聚类的结果,而是以若干神经元同时并行反映聚类结果。在某一个外界信息所引起的并不是对一个神经元的兴奋性刺激,而是对某一个神经元为中心的一个区域神经元的兴奋刺激,并且这种刺激的强度不是均一的,有强弱之分。刺激的趋势与强度呈墨西哥草帽的形状,神经元受兴奋刺激的强度,以区域中心为最大,伴随着区域半径的增大,强度逐渐减弱,远离区域中心的神经元相反要受

到抑制的作用,这就是为什么把输出层安排在一个二维的网格上的原因。为了刻画这个区域自组织神经网络引入了拓扑邻域的概念。

当邻域的半径为 0 时,邻域仅仅包括获胜神经元;而半径为 1 时,邻域包括除了获胜神经元之外的 8 个邻近神经元。当半径增大时,邻域依此规律放大。

自组织映射学习算法的具体步骤如下:

(1)$X(n)=[x_1(n),x_2(n),\cdots,x_N(n)]^T$ 为输入向量,或称训练样本。设置总迭代次数为 k。$W_i(n)=[w_{i1}(n),w_{i2}(n),\cdots,w_{iN}(n)]^T$ 为权值向量,$i=1,2,3,\cdots,M$。M 是输出层神经元的个数。

(2) 初始化:将权值向量 W_i 用小的随机数进行初始化,设置初始学习速率 $\eta(0)$,$N_c(0)$。

(3) 采样:从输入空间中选取训练样本 X'。

(4) 近似匹配:通过欧氏距离最小的标准:$\|X'-W_c'\|=\min\|x'-W_i'\|$,$i=1,2,3,\cdots,M$,来选取获胜神经元 c,实现神经元的竞争过程。

(5) 对于获胜的神经元 c,求得对应获胜邻域 $N_c(n)$。对输出层中神经元的连接权矢量进行调整,调整算法如下:

$$W_i(n+1)=\begin{cases}W_i(n)+\eta(n)[X_k-W_i(n)], i\in N_c(n)\\ W_i(n),\text{其它}\end{cases}$$

(6) 更新学习速率 $\eta(n)$ 及拓扑领域:

$$\eta(n)=\eta(0)(1-\frac{n}{N})$$

$$N_c(n)=\mathrm{INT}[N_c(0)(1-\frac{n}{N})]$$

判断迭代次数是否超过 k,如果 $n\leqslant k$,转到(3);否则,结束迭代。

经过上面算法的处理,对训练的数据进行了初步的聚类,神经网络形成了关于正常与异常的初步模式,下面在利用 LVQ 对初步形成的模式在有监督的情况下再进行分类,使模式更加清晰。

1.4 学习矢量化(LVQ)

学习矢量量化算法属于有监督竞争学习算法。能够弥补 SOM 无监督学习的不足,在网络学习中,允许对输入被分配到哪一类进行指定。

1.4.1 LVQ 网络模型

学习矢量量化网络和自组织映射网络具有非常类似的结构,网络同样有输入和输出两层组成,但是在输出层中将 M 个神经元呈一维线性排列。LVQ 没有在输出层引入拓扑结构,因此在网络学习中也不再有获胜邻域的概念。其网络结构如图 4 所示。

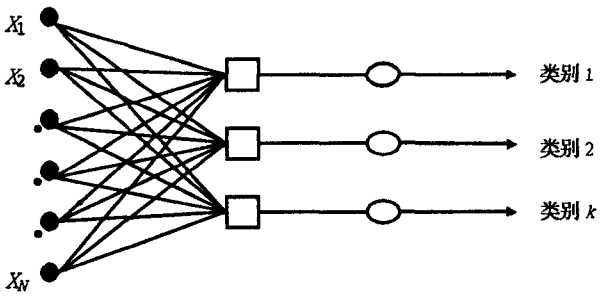

图 4 LVQ 网络结构图

LVQ 根据输入向量和权值向量的最小欧氏距离选取获胜神经元,并且采用优胜劣汰的竞争机制,令该神经元的输出为 1,其它神经元的输出为 0。并且学习速率随迭代次数的增加而减小。

1.4.2 LVQ 学习算法

(1)设置变量和参量图:

$\boldsymbol{X}(n)=[x_1(n),x_2(n),\cdots,x_n(n)]^T$ 为输入向量,或称训练样本。

$\boldsymbol{W}_i(n)=[w_{i1}(n),w_{i2}(n),\cdots w_{in}(n)]^T$ 为权值向量,$i=1,2,3,\cdots,M$。M 是输出层神经元的个数。选择学习速率函数 $\eta(n)$,n 为迭代次数,N 为迭代总次数。

(2) 初始化:初始化权值向量 $\boldsymbol{W}_i(0)$ 及学习速率 $\eta(0)$。

(3) 采样:从输入空间中选取训练样本 X。

(4) 寻找获胜神经元 C:通过欧氏距离最小的标准:$\|X'-W_c'\|=\min\|x'-W_i'\|$

(5) 判断分类是否正确,根据以下规则调整获胜神经元的权值向量:

用 Lw_c 代表与获胜神经元权值向量相联系的类,用 Lx_c 代表与输入向量相联系的类。如果 $Lx_c=Lw_c$,则 $W_c(n+1)=W_c(n)+\eta(n)[X-W_c(n)]$。否则,当 $Lx_c\neq Lw_c$ 时,有 $W_c(n+1)=W_c(n)-\eta(n)[X-W_c(n)]$。对于其它神经元保持不变。

(6) 调整学习速率 $\eta(n)$:

$\eta(n)=\eta(0)(1-n/N)$ 判断迭代次数是否超过 k,如果 $n\leqslant k$,转到(3);否则,结束迭代。

2 实验分析

为检验文中提出的方案,在 LINUX 环境下搭建测试平台。

主要对二级异常检测模块进行测试。系统服务程序 lpr 是一个提供远程打印服务的系统程序,它存在缓冲区溢出漏洞,容易被攻击者利用来执行具有 root 权限的 shell 程序。在一级的误用检测模块中 Snort 已对缓冲区溢出的攻击已有规则,为了测试异常检测的能

力,取消了 Snort 对缓冲区溢出的规则。

为了使系统缓冲区溢出,被用来攻击的字符串总长度应达到 4096 个字符以上。由于攻击程序所产生的字符串的最后一部分是真正产生攻击的。因此,取攻击字符串的最后 75 个字符作为导致程序异常行为的程序输入来训练神经网络。另一方面,正常的 lpr 输入字符串一半长度不长于 75 个字符,因此,以输入的前面的 75 个字符作为程序正常行为的输入来训练神经网络。

所以,神经网络的输入层节点个数为 75,根据仿真实验使用输出层的神经元的个数为 20 * 20 个。

实验中,共获得数据 2000 份,其中有 600 份是导致程序异常的数据,将数据平均分为两部分,每一部分包含 300 份异常数据,拿出其中的一个部分作为训练神经网络,剩下的一部分用来检验神经网络,试验的结果如表 1 所示。

表 1　神经网络算法数据对比

	BP	SOM	SOM+LVQ
检测率	86.1%	90%	94%
误报率	22%	18%	14%

经过试验数据的比较,发现:

1)文中的混合神经网络算法相对于传统的 BP,SOM 正确率有所提高。

2)混合神经网络可以有效地应用专家指导信号。SOM 网络先前的聚类可以减少 LVQ 的训练时间。国内的一些技术虽然也能达到较高的检测率,但是以较长的训练时间为代价的。

3)本方法仍有较高的虚报率,在于先前训练的数据还不能够完全反映系统服务程序 lpr 被攻击的行为,所以算法需要在数据的选择方面加以改进。

3　结束语

入侵检测的误用检测,作为早期的主流检测技术,一直以它的高速来获得人们的青睐,但由于新型入侵技术的日益增加,误用检测已无法单独保护现在的网络安全。异常检测优势在于能够检测出以前没有检测出的入侵,与误用检测不同的是,异常检测的模式库需要利用程序以前的运行行为来自动的建立,需要庞大的训练样本。其核心在于对以前程序的行为类的边界是否明晰,但是现有的技术是无法完全将现有攻击技术通过异常检测技术训练成模式。

文中将误用检测和异常检测相结合,通过 Snort 检测已知的入侵行为,然后根据 SOM 算法对网络数据先聚类,再利用 LVQ 在聚类的基础上分类的方法,使分类的边界更加明晰,试验证明混合入侵检测系统在防御已知网络攻击和检测未知攻击上都有了明显的提高。

参考文献:

[1] Chenfeng Vincent Zhou. A Survey of Coordinated Attacks and Collaborative Intrusion Detection[J]. Computers & Security, 2009(6):1-17.

[2] 张　铮. 改进贝叶斯分类算法在入侵检测中的研究[J]. 计算机技术与发展,2007,17(1):174-176.

[3] Schultz E E. The Future of Intrusion Prevention[J]. Computer Fraud & Security,2007(8):11-13.

[4] Ganame A K. A Global Security Architecture for Intrusion Detection on Computer Networks[J]. Computers & Security, 2008(3):30-34.

[5] 青华平. 基于模式匹配和神经网络的分布式入侵防御系统的研究[J]. 计算机安全,2006(2):33-35.

[6] 廖光忠. 基于 Linux 的网络入侵防御系统的研究和设计[J]. 计算机技术与发展,2008,18(6):134-136.

[7] 张广斌. 基于神经网络的入侵防御系统研究[J]. 微计算机信息,2007,24:64-66.

[8] 孙吉贵. 聚类算法研究[J]. Journal of Software, 2008, 19(1):48-61.

(上接第 140 页)

[7] 王天亮,陈　刚,徐宏炳. 基于共享数据库的数据共享技术[J]. 计算机工程与设计,2007,28(8):1923-1926.

[8] 汪明申,王　强. Mashup 系统构建研究[J]. 现代图书情报技术,2009(5):34-38.

[9] 廖建尚. 论 Mashup 技术与传统系统集成方案的异同[J]. 电脑知识与技术,2009,12(4):3249-3250.

[10] 邓启辉,赵　英. RIA 技术在数字图书馆中的应用[J]. 图书馆学研究,2008(6):27-30.

[11] Shanahan F. Mashups Web2.0 开发技术[M]. 吴宏泉译,北京:清华大学出版社,2007:129-150.