第 33 卷 第 9 期 计 算 机 工 程 2007 年 5 月
Vol.33 No.9 Computer Engineering May 2007
·安全技术· 文章编号：1000—3428(2007)09—0160—03 文献标识码：A 中图分类号：TP301.6

基于融合免疫算法和 RBF 网络的入侵检测系统

史长琼[1,2]，陈 旭[1]，唐贤瑛[1]
(1. 长沙理工大学计算机与通信工程学院，长沙 410076；2. 湖南大学计算机与通信工程学院，长沙 410082)

摘 要：入侵检测技术是网络信息安全技术中很重要的一个研究领域。为了提高入侵检测系统对入侵类型的识别能力，在该系统中将免疫算法与 RBF 网络融合起来，形成一种双层分类结构。试验结果表明，基于融合免疫算法和 RBF 网络的入侵检测系统能有效地区分 4 种入侵类型。

关键词：入侵检测；免疫算法；RBF 网络；双层分类

Intrusion Detection System Based on Combination of Immune Arithmetic and RBF Network

SHI Changqiong[1,2], CHEN Xu[1], TANG Xianying[1]
(1. College of Computer and Communication Engineering, Changsha University of Science & Technology, Changsha 410076;
2. College of Computer and Communication Engineering, Hunan University, Changsha 410082)

【Abstract】 Intrusion detection technology is a very important research field on network and information security technology. In order to improve the distinguish capability of intrusion detection system, immune arithmetic and RBF network are combinated in the intrusion detection system, which is a double-layer classifiable structure. Experimental results show that the intrusion detection system based on the combination of immune arithmetic and RBF network can efficiently distinguish four attack types.

【Key words】 Intrusion detection; Immune arithmetic; RBF network; Double-layer classification

1 概述

入侵检测技术是近 20 年来出现的一种主动保护自己以免受黑客攻击的新型网络安全技术，被认为是防火墙之后的第 2 道安全闸门，它在不影响网络性能的情况下对网络进行检测，从而提供对内部攻击、外部攻击和误操作的实时保护。

1987 年乔治敦大学的Dorothy Dennings提出了入侵检测专家系统(Intrusion Detection Expert System, IDES)模型，这是基于主机的入侵检测系统，它将主机的审计记录和日志文件与入侵规则库进行模式匹配来检测入侵，这样的检测模型很难应付当前庞大的网络环境，有很高的漏报率与误报率。于是在 1990 年，加州大学戴维斯分校的L T Heberlein等人提出了基于网络的入侵检测(Network Security Monitor, NSM)这一概念。后来，Kim和Bentley又提出了现代网络入侵检测系统应当有分布性、自适应性和低消耗性 3 个特性[1]。

近几年来，入侵检测的新方法主要有Forrest等人将免疫原理运用到分布式入侵检测领域[2]；李鸿培等人利用神经网络来进行分类；Ross Anderson 和Abida Khattak将信息检索技术引入到入侵检测；W.Lee从信息论的角度探讨了入侵检测的实现问题。对于入侵检测系统中入侵类型识别技术，大部分都是通过神经网络实现，如反向传播(Back Propagation, BP)网络、径向基函数 (Radial Basis Function, RBF)网络、RBF二叉神经树，组合RBF网络等。在入侵检测系统中，如果仅仅采用免疫算法，只能判断数据是正常还是异常，而很难识别出异常数据属于哪类入侵，也就不能及时调用相应的报警处理模块；而仅仅采用神经网络进行入侵类型的识别，则所有待检测数据都要通过神经网络来处理，就增加了时间复杂度。本文所建立的网络入侵检测系统模型是将免疫算法与RBF网络融合起来，形成一种双层分类结构，它不仅能区分正常与异常的网络数据，而且能识别所发生的具体入侵类型，这样就能针对具体入侵进行报警，处理等一系列的响应。该系统应用于KDD Cup 1999 Data中，通过试验能很好地识别出待检测数据中入侵数据，并能区分出具体的入侵类型。

2 免疫算法与 RBF 神经网络的融合

本文所设计的网络入侵检测系统的模型如图 1 所示，系统采用一种双层分类结构，首先利用免疫算法将网络数据区分成“ Self ”(自身)与“ NonSelf ”(非自身)两类数据，这是第 1 层分类；然后将“ NonSelf ”数据输入到 RBF 神经网络进行入侵类型分类，这是第 2 层分类。

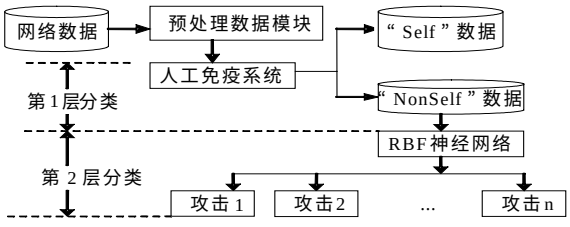

图 1 融合免疫算法和 RBF 网络的入侵检测系统的结构

基金项目：湖南省教育厅自然科学基金资助项目(05C245)；湖南省自然科学基金资助项目(00JJY2059)
作者简介：史长琼(1968－)，女，副教授、在职博士生，主研方向：网络信息安全，人工智能；陈 旭，硕士生；唐贤瑛，教授
收稿日期：2006-05-26 **E-mail：**shi.changqiong@163.com

2.1 免疫算法

在免疫算法中非常典型的算法就是Forrest提出的否定选择算法[3,4]，它定义“ Self ”为被检测系统的正常模式，检测系统将随机产生的模式(称为未成熟检测元)与大量的被检测系统的正常模式按照一定的匹配算法相匹配。如果匹配成功，说明该未成熟的检测元与被检测系统的正常模式吻合，那么该未成熟的检测元将被移除，不能成为成熟检测元；反之，它将成为成熟检测元。然后将这些训练成熟的检测元与待检测元进行模式匹配，如果匹配成功，说明它属于“ NonSelf ”，有异常模式产生。本文所设计的系统将沿用这套思想，将待检测数据区分成“ Self ”和“ NonSelf ”两类，进行第 1 层分类。

2.2 RBF 网络

RBF神经网络是由Moody和Darken提出来的[5]，它是一种单隐层的 3 层(输入层、隐层、输出层)前馈人工神经网络模型。RBF神经网络的结构，见图 2。

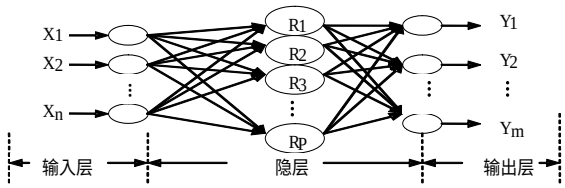

图 2 RBF 神经网络结构

输入层的每一个神经元对应于输入向量 x 的 1 个分量，每个输入神经元到隐层神经元都是全互连的，连接权值固定不变，均为 1。隐层是最关键的一层，它的激励函数最常用的是高斯函数，即

$$R_i(x) = \exp(-\| x - c_i \|^2 / 2\sigma_i^2), \text{i=1,2,...,p}$$

其中，x 是 n 维输入向量；Ci 是第 i 个基函数的中心，与 x 具有相同维数的向量；σ_i 是第 i 个感知的变量，它决定了该基函数围绕中心点的宽度；p 是隐层的单元个数(隐含层节点数)。$\| x - c_i \|^2$ 是向量 x-Ci 的范数，它通常表示 x 与 Ci 之间的距离；$R_i(x)$ 在 Ci 处有一个唯一的最大值，随着 $\| x - c_i \|^2$ 的增大，$R_i(x)$ 迅速衰减到零。

对于给定的输入 x∈Rn，只有一小部分靠近 x 的中心被激活。基函数的中心调整算法采用 K 均值聚类算法，引入了竞争机制。

输出层对应于模式类别向量空间，它的激励函数一般为纯线性函数。输出单元 j 的输出为

$$y_j = \sum_{i=1}^{k} w_{ij} R_i(x), \quad \text{j=1,2,...,m}$$

其中，w_{ij} 表示第 i 个中间层神经元和第 j 个输出神经元之间的权值，这个权值是可调的，它的调整算法采用最小均方(Least Mean Square, LMS)算法。

本文设计的入侵检测系统通过这样的RBF网络进行数据的第 2 层分类，即将第 1 层分类后得到的“ NonSelf ”输入到RBF网络，识别出异常数据中具体入侵类型。根据Amoroso[6]给出的一个攻击分类方法应满足的分类标准，即互斥性、完备性、非二义性、可重复性、可接受性和实用性 6 个特性。

该系统将攻击类型分为 4 种主要类型：DoS(Denial of Service)，R2L(unauthorized access from a remote machine)，U2R(unauthorized access to local superuser root privileges)，probing(surveillance and other probing)。

3 融合免疫算法和 RBF 网络的入侵检测系统的算法

3.1 数据预处理

本文建立的入侵检测系统的试验数据是 KDD Cup 1999 Data 的数据。本实验中采用了 1/10 数据集的部分数据，根据对这些数据的分析，将这些数据进行两部分处理。

(1)从 41 个属性中提取了其中具有代表性的 21 个属性。如表 1 所示，对基本属性中的protocol_type即协议类型要进行分析[7]，在建立双层分类器前，首先对数据包的协议进行分析，然后根据每一类协议的特点分别进行特征提取和选择。

表 1 属性列表

基本属性	duration, protocol_type,service, flag ,src_bytes, dst_bytes, urgent
主要属性	hot,logged_in,num_compromised, root_shell,num_root,is_guest_login
流量属性	count,serror_rate,rerror_rate,same_srv_rate, diff_srv_rate,srv_count,srv_serror_rate,srv_rerror_rate, srv_diff_host_rate

(2)将属性的取值进行区间化处理在这些属性取值有离散型数据和符号型数据，如果是离散型数据，将其化为区间值，对每一段区间值进行相应的整数编码；如果是符号型数据，对每种符号型数据进行整数编码。

3.2 第 1 层分类的算法设计

第 1 层分类由否定选择算法来实现，自身集 N_s =2 048，匹配函数为 f(x，y)，匹配法则按位异或(XOR(x,y))求距离评分方法，即计算 x 与 y 的相似程度，该相似程度作为匹配分数(Score)，如果 Score 大于某个数，则 f(x,y)值为 1，表示匹配成功，否则 f(x,y)值为 0，表示匹配失败。匹配分数计算方法为

Score=XOR(x,y)

第 1 层分类的算法具体描述如下:

初始化 D(成熟检测元的集合)为空；

(1)求出整个系统需要的未成熟检测元(N_{R_0})的个数为

$$N=N_{R_0}=-\ln(P_f)/(P_m(1-P_m)^{N_s})$$

其中，P_f表示未能检测到入侵的概率，P_m表示与自身数据集成功匹配的概率，N_s表示自身数据集。

(2)for i=0:N-1；

(3)随机生成一组未成熟检测元 xi；

(4)将 xi 与 Self 的每个模式 s 采用匹配分数计算方法，计算匹配分数 Score；

(5)if(Score<m)　f(xi,s)=0；

(6)将 xi 写入集合 D 中；

(7)else f(xi,s)=1；

(8)end

(9)end　//得到成熟检测元集合(NR)

(10)初始化 N(NonSelf 集合)为空；

(11)输入待检测元集合(NT)中的一组数据 t；

(12)将 t 与 D 中的每个模式 d 匹配，计算出匹配分数 Score；

(13)if(Score>m)　f(t,d)=1；

(14)将 x 写入集合 N 中；

(15)else f(t,d)=0；

(16)end　//得到 NonSelf 集合

3.3 第 2 层分类的算法设计

第 2 层分类是通过 RBF 网络实现的，该网络的输入层的输入数据为第 1 层分类后的 NonSelf 集合中的数据。

RBF 网络隐层的激励函数采用高斯函数，它由聚类中心和聚类宽度确定，中心调整采用 K 均值聚类算法，对训练模式进行聚类，每一类对应一个神经元。K 均值聚类算法是一种在线自适应聚类学习算法，不需要事先确定隐含层单元的

个数，完成聚类所得到的 RBF 网络是最优的。具体步骤如下:

(1)选择一个适当的高斯函数宽度 r，定义一个矢量 A(l)用于存放属于各类的输出矢量之和，定义一个计数器 B(l)用于统计属于各类的样本个数，其中 l 为类别数。

(2)从第 1 个数据对(X1,Y1)开始，在 X1 上建立一个聚类中心，令 C1= X1，A(1)= Y1， B(l)=1。

(3)考虑第 2 个样本数据对(X2,Y2)，求出 X2 到 C1 这个聚类中心的距离‖X2- C1‖。

if ‖X2- C1‖≤r C1 为 X2 的最近邻聚类，且令 A(l)= Y1+ Y2, B(l)=2, w1= A(l)/ B(l)；

else 将 X2 作为一个新的聚类中心，并令 C2= X2, A(2)= Y2, B(2)=1

(4)本文考虑第 k 个样本数据对(Xk, Yk)(k=3,4,...,N)时，存在 P 个聚类中心，其中心点分别为 C1,C2,...,CP，在上述建立的 RBF 网络中已有 P 个隐单元。再分别求出 XK 到这 P 个聚类中心的距离

‖XK- Ci‖,i=1,2,...,P，设‖XK- Cj‖为这些距离中的最小距离，即 Cj 为 XK 的最近邻聚类，则:

if‖XK- Cj‖>r，则将 XK 作为一个新聚类中心。令 Cp+1=Xk,P=P+1, A(P)= YK, B(P)=1，并保持 A(i)、B(i)的值不变，i=1,2...,P-1

else A(j)= A(j)+ Yk, B(j)= B(j)+1。当 i≠j 时，i=1,2,...,P，保持 A(i)、B(i)的值不变。隐单元到输出层的权矢量为 wi=A(i)/ B(i),i=1,2,...,P

(5)根据上述规则建立的 RBF 网络其输出应为

$$f(x_k)=[\sum_{i=1}^{P} w_i \exp(-\|x_k-c_i\|^2/r^2)]/[\sum_{i=1}^{P}\exp(-\|x_k-c_i\|^2/r^2)]$$

输出层的单元个数为 4 个，即 4 种入侵类型(DoS、R2L、U2R、probing)进行相应的编码。

4 试验分析

该系统通过 Matlab 7.0 进行算法设计编写并运行测试，测试结果比较如下。

比较策略 1 首先将检测数据只输入到 RBF 网络进行分类得到结果 1，然后将同样的检测数据先通过免疫算法进行第 1 层分类，再将第 1 层分类后得到的异常数据输入到 RBF 网络进行第 2 层分类，这样的双层分类后得到结果 2，将结果 1 与结果 2 进行比较。结果如表 2。

表 2 中误报率表示将正常行为识别成入侵行为的比率，漏报率表示将入侵行为识别成正常行为的比率，检测率表示对入侵行为正确检测的比率。由表 2 中的结果可看出，本文采用的双层分类结果比只采用 RBF 网络进行分类后结果要好。

表 2 策略 1 结果

	误报率	漏报率	检测率
结果 1	0.016 3	0.033 4	0.958 3
结果 2	0.013 5	0.027 6	0.972 6

比较策略 2 将“仅采用 RBF 网络对 4 种入侵类型的识别率”与“融合后的双层分类结构对 4 种入侵类型的识别率”比较。结果如表 3。

表 3 策略 2 结果

	DoS	R2L	U2R	probing
仅采用 RBF 网络	0.887 5	0.914 3	0.925 6	0.898 5
双层分类结构	0.936 7	0.964 6	0.978 5	0.945 3

表 3 中的数据均为识别率，它表示对入侵类型的正确识别的比率。由表 3 中结果可看出，采用双层分类结构的入侵检测系统对 4 种入侵类型识别效果更好，而且在运行时间上比仅采用 RBF 网络要快。

5 小结及进一步工作

本文提出的基于融合免疫算法和 RBF 网络的入侵检测系统，形成一种双层分类的结构。通过试验分析，该系统能在比较短的时间内，有比较高的检测率，较好地区分 4 类入侵。进一步工作是将对成熟检测元进行优化，将 RBF 网络训练得更加完美，提高该系统的检测率，降低误报率和漏报率。

参考文献

1 罗守山. 入侵检测[M]. 北京: 北京邮电大学出版社, 2004.

2 Forrest S, Hofmery S A, Somayaji A. Computer Immunology[J]. Communications of the ACM, 1997, 40(10): 88-96.

3 Forrest S, Perelson A, Allen L. Self-nonself Discrimination in a Computer[C]//Proceedings of IEEE Symposium on Research in Security and Privacy. 1994: 202-212.

4 Yao Guangwei, De Lingzheng, Ying Wang. Research of a Negative Selection Algorithm and ITS Application in Anomaly Detection[C]// Proceedings of the 3rd International Conference on Machine Learning and Cybemetics. 2004: 2910-2913.

5 张建宝, 慈林林, 赵宗涛. RBF 网络分类器的实现及应用[J]. 计算机工程与科学, 2001, 23(6): 105-107.

6 王晓程, 刘恩德, 谢小权. 攻击分类研究与分布式网络入侵检测系统[J]. 计算机研究与发展, 2001, 38(6): 727-734.

7 张 莉, 孙 钢, 郭 军. 基于特征分析的多分类器融合的网络入侵检测[J]. 计算机工程与应用, 2004, 40(18): 13-22.

（上接第 159 页）

5 Ateniese G, Blundo C, De Santis A. Constructions and Bounds for Visual Cryptography[C]//Proc. of the 23rd International Colloquium on Automata, Languages and Programming. 1996.

6 Blundo C, De Santis A, Stinson D R. On the Contrast in Visual Cryptography Schemes[J]. Journal of Cryptology, 1999, 12(4): 261-289.

7 Hou Y C, Tu S F. Visual Cryptography Techniques for Color Images without Pixel Expansion[J]. Journal of Information Technology and Society, 2004, 4(1): 95-110.

8 Franklin M F. Cyclic Generation of Orthogonal Latin Squares[J]. Ars Combinatoria, 1984, 17(1): 129-140.

9 Ateniese G, Blundo C, De Santis A. Extended Capabilities for Visual Cryptography[J]. Theoretical Computer Science, 2001, 250(1/2): 143-161.

10 Blundo C, Darco P, De Santis A. Contrast Optimal Threshold Visual Cryptography Schemes[J]. Discrete Mathematics, 2003, 16(2): 224-261.