CN 43-1258/TP
ISSN 1007-130X

计算机工程与科学
Computer Engineering & Science

第 36 卷第 8 期 2014 年 8 月
Vol. 36, No. 8, Aug. 2014

文章编号:1007-130X(2014)08-1469-07

基于自适应进化神经网络算法的入侵检测*

杨宏宇,赵明瑞,谢丽霞

(中国民航大学计算机科学与技术学院,天津 300300)

摘　要:针对目前多数入侵检测系统的低检测率问题,提出一种自适应进化神经网络算法 AENNA。基于遗传算法和 BP 神经网络算法,利用模拟退火算法的概率突跳和局部搜索强的特性对遗传算法进行改进,采用双种群策略的遗传进化规则实现 BP 神经网络权值和结构的双重优化;通过对遗传算法的交叉算子与变异算子的改进,设计一种自适应的神经网络训练方法。实验结果表明,基于 AENNA 的入侵检测方法能够有效提高系统的检测率并降低误报率。

关键词:遗传算法;神经网络算法;模拟退火算法;入侵检测

中图分类号:TP393.08　　**文献标志码**:A

doi:10.3969/j.issn.1007-130X.2014.08.008

Intrusion detection based on the adaptive evolutionary neural network algorithm

YANG Hong-yu, ZHAO Ming-rui, XIE Li-xia

(School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China)

Abstract: Aiming at the problem of low detection rate existed in current intrusion detection systems, an adaptive evolutionary neural network algorithm (AENNA) based on the genetic algorithm and the BP algorithm is proposed. Firstly, considering the characteristic of probabilistic jumping property and local search ability in the simulated annealing algorithm, the genetic algorithm is improved. Secondly, using the dual population evolution rule, the algorithm optimizes the weight and the network structure of the BP neural network simultaneously. An adaptive neural network training method is designed through improving the crossover operator and mutation operator of the genetic algorithm. Experimental results show that the AENNA based intrusion detection method can effectively improve the detection rate and reduce the false positive rate.

Key words: genetic algorithm; neural network; simulated annealing algorithm; intrusion detection

1　引言

当今社会,随着网络技术和网络规模的不断发展,针对网络和计算机系统的攻击变得越来越频繁,攻击手法也复杂多样。而传统的入侵检测技术由于技术自身的局限和不足已无法满足安全高度敏感部门的需求,研究人员对诸如神经网络技术、专家系统、机器学习和进化算法等智能方法在入侵检测中的应用开展了大量研究,为入侵检测领域的研究开启了一个崭新的方向[1]。

文献[2]在基于最小闭包球的支持向量机算法的基础上,提出了基于广泛内核的最小闭包球算法的入侵检测方法,但该方法无法高效处理多类问题且范围限制严格。文献[3]提出一种基于关联决策的网络多源入侵检测算法,该算法运用模糊识别手

* 收稿日期:2012-12-30;修回日期:2013-04-03
基金项目:国家自然科学基金资助项目(60776807,61179045);国家 863 计划资助项目(2006AA12A106);天津市科技计划重点项目(09JCZDJC16800);中国民航科技基金(MHRD201009,MHRD201205);中央高校基本科研业务费专项(ZXH2009A006)
通信地址:300300 天津市东丽区中国民航大学(北区)6#民航信息技术科研基地
Address: IT Science and Research Base of CAAC, 6#, Civil Aviation University of China (North Campus), Dongli District, Tianjin 300300, P. R. China

段,通过计算各个多源子攻击的关联度,对入侵行为进行模糊差异聚类,完成入侵检测,但过于依赖参数特征的计算准确性,对预分类的结果影响较大。文献[4]提出一种神经网络专家系统模型,并将该模型应用于入侵检测系统,通过关联检测性能的方法扩充了单一系统的检测能力,但该模型也增加了检测时间,时间复杂度偏高。文献[5]提出一种自适应遗传算法,该算法首先考虑个体适应度的变化,并将交叉和变异概率在最大适应度与平均适应度之间作线性变换,但该算法在演化初期,较优个体几乎不发生变化,因此容易走向局部收敛。文献[6]提出一种改进的自适应遗传算法,并有效地应用到非线性系统的参数辨识问题上,但该算法中的局部较优个体不易被淘汰,全局搜索能力不强,且对于分布偏多于平均适应度范围的种群演化容易停滞不前。

传统神经网络算法的收敛速度较慢;遗传算法局部搜索能力差但全局搜索能力却很强;模拟退火算法具有强收敛及概率突跳的特性。本文基于智能互补融合的观点,将遗传算法、模拟退火算法和神经网络结合提出一种自适应进化神经网络算法AENNA(Adaptive Evolutionary Neural Network Algorithm)。

2 神经网络改进进化算法

2.1 改进算法设计思路

传统BP算法虽然具有简单和可塑的优点,但由于BP算法本质上是采用梯度下降搜索方法,因而不可避免地存在固有的不足,如易陷入误差函数的局部极小点,而且对于较大搜索空间、多峰值和不可微函数等问题也不能有效搜索到全局极小点。而遗传算法是克服这一不足的有效解决办法,主要是由于遗传算法是一种全局优化搜索算法,因而能够避开局部极小点,而且在进化过程中无需提供所要解决问题的梯度信息。另一方面,标准遗传算法易出现未成熟收敛现象,虽然相应的改进方法很多,如调整操作参数、增加种群规模等,但都没有考虑使改进后的算法具有学习能力和鲁棒特性,这恰是神经网络的优势所在。因此,本文提出一种自适应进化神经网络算法(AENNA),通过改进遗传算法,优化BP神经网络的连接权值与网络结构,应用于BP神经网络的训练。

鉴于传统遗传算法个体的多样性下降过快,影响遗传算法通过交叉和变异跳出局部最优的能力,本文采用双种群遗传策略。此策略属于并行遗传策略,即同时进行多种群的进化,这种策略的优点在于可以改变种群内停滞的局面,在交换不同种群中优秀个体遗传信息的同时,能够跳出局部最优,这也加快了算法的进化速度。

用一个类来表示群体中的每个个体,同一种群的不同个体具有不同的隐含层数、节点数和连接权值。大种群中每个个体都来自一个小种群,小种群中所有个体均具有相同的网络结构、不同的连接权值。不同小种群中的个体在群体内进化,小种群中适应度较高的个体则有较大概率进入大种群进行交叉和变异操作,而后回到原小种群进行下一次的小群体内部进化。小种群中的进化操作选用调整的自适应交叉算子和变异算子,大种群中的进化操作则采用调整的增加算子和删除算子。

考虑到模拟退火算法在解决大型优化组合问题上的有效性,本文将其引入到对遗传算法的改进中,结合遗传算法群体并行搜索能力和模拟退火概率突跳特性来改善优化效率并避免局部极小的可能性。

遗传算法中交叉算子和变异算子对于遗传算法解空间的影响较大,这是由于交叉算子会造成染色体局部相似,交叉概率偏大会破坏适应度值高的个体,偏小则容易让算法停滞;同样,变异概率过大则变成了纯粹的随机搜索,过小则会导致无法驱动搜索转向其他解空间,而无法接近最优解。在参考了文献[5,6]提出的自适应遗传算法的基础上,本文从小种群的交叉算子和小种群变异算子两方面对遗传算法进行改进。

2.2 小种群交叉算子

小种群选用调整自适应交叉算子进行种群个体间的交叉。根据种群适应度值的大小,逐渐地调整整个种群的交叉概率。调整后的交叉概率 P_c 的计算公式[6]为:

$$P_c=\begin{cases}k_2-\dfrac{(k_2-k_1)(f'-f_v)^2}{(f_a-f_v)^2}, & f'\geqslant f_v\\ k_3-\dfrac{(k_3-k_2)(f'-f_i)^2}{(f_v-f_i)^2}, & f'<f_v\end{cases} \tag{1}$$

其中,f_a 表示最大适应度值,f_i 表示最小适应度值,f_v 表示平均适应度值,这三个值用来表示种群适应度的集中程度,使 P_c 随适应度值在 f_a、f_i 和 f_v 之间进行变化。f' 为待交叉的两个个体中较大的适应度值。公式中 $k_1=0.6$,$k_3=0.9$,k_2 在(k_1,k_3)间取值。适应度函数为:

$$F=\frac{1}{1+E},$$

$$E=\sqrt{\sum_{k=1}^{N}\sum_{t=1}^{N}(o_k(t)-y_k(t))^2} \tag{2}$$

其中,F 为适应度函数值,取值在[0,1]之间;E 为误差函数值;N 为训练样本总数;$o_k(t)$表示期望输出;$y_k(t)$表示网络的实际输出[7]。

对于个体的选择,采用高适应度值、高概率中选方法将个体从父代中选出,其中概率 p_i 的计算公式[8]为:

$$p_i=\frac{f_i}{\sum_{i=1}^{N}f_i},i=1,2,\cdots,N \tag{3}$$

据此,将个体的积累概率定义为 $\hat{p}_i$:

$$\hat{p}_i=\sum_{k=1}^{i}p_k,i=1,2,\cdots,N \tag{4}$$

在上述运算基础上,运用调整后的交叉概率 P_c 种群中的个体进行交叉操作。由于实数编码方式精度高且便于大空间搜索,故本文采用实数编码方式并运用两点交叉方法,对编码后的染色体实施交叉操作,设 $X_1=(x_1^1,x_2^1,\cdots,x_n^1)$,$X_2=(x_1^2,x_2^2,\cdots,x_n^2)$是两个染色体,在第 i 点到第 j 点实施交叉产生后代为[9]:

$$\begin{cases}Y_1=(x_1^1,x_2^1,\cdots,x_{i-1}^1,y_i^1,\cdots,y_j^1,x_{j+1}^1,\cdots,x_n^1)\\ Y_2=(x_1^2,x_2^2,\cdots,x_{i-1}^2,y_i^2,\cdots,y_j^2,x_{j+1}^2,\cdots,x_n^2)\end{cases} \tag{5}$$

其中,子代 Y_1 中的元素 y_k^1 和子代 Y_2 中的元素 y_k^2 $(i\leqslant k\leqslant j)$由式(6)组合产生,假设 $x_k^1=a$,$x_k^2=b$,则:

$$\begin{cases}y_k^1=x_k^1\cdot\dfrac{a^2+b^2}{(a+b)^2}+x_k^2\cdot\dfrac{2ab}{(a+b)^2},i\leqslant k\leqslant j\\ y_k^2=x_k^2\cdot\dfrac{a^2+b^2}{(a+b)^2}+x_k^1\cdot\dfrac{2ab}{(a+b)^2},i\leqslant k\leqslant j\end{cases} \tag{6}$$

由于模拟退火法能有效解决大规模的组合优化问题,所以运用模拟退火机制[10]对交叉后生成的子代进行取舍,具体步骤设计为:

步骤 1 依据式(5)和式(6)对父代个体 X_1、X_2 进行交叉,生成子代个体 Y_1、Y_2,按照式(2)计算子代个体的适应度值 $F(Y_1)$、$F(Y_2)$。

步骤 2 若 $F(Y_1)>F(X_1)$ 且 $F(Y_2)>F(X_2)$,则子代个体 Y_1 取代父代个体 X_1,子代个体 Y_2 取代父代个体 X_2,转向步骤 4;否则,若子代个体的适应度值小于父代个体的适应度值,则进行步骤 3 操作。

步骤 3 在[0,1]产生随机数 β,计算 $\Delta=F(X)-F(Y)$,其中,X 为父代的个体,Y 为子代个体;

$$T_0=-d/\log\alpha$$

其中,T_0 为初始温度,d 为初始种群个体间适应度的最大差值,α 取 0.01;$T_i=T_0(0.99i-1)$,其中,i 为进化代数;

$$Prob=\min(1.0,\exp(-\Delta/T_i))$$

若 $Prob\geqslant\beta$,则子代个体 Y 取代父代个体 X;否则保留父代个体 X。

步骤 4 输出取舍后的个体。

2.3 小种群变异算子

小种群采用调整自适应变异算子进行个体变异操作。变异概率依据适应度值的集中程度自适应地变化,通过设置参数区间来限制变异概率的取值范围,可有效保证变异操作的合理性,调整后的变异概率 P_m 计算公式[9]为:

$$P_m=\begin{cases}k_1-\dfrac{(k_1-k_2)(f-f_i)^2}{(f_v-f_i)^2},f<f_v\\ k_2-\dfrac{(k_2-k_3)(f-f_v)^2}{(f_a-f_v)^2},f\geqslant f_v\end{cases} \tag{7}$$

其中,f_a、f_v 和 f_i 分别代表种群中的最大适应度值、平均适应度值和最小适应度值;f 为待变异的个体适应度值;$k_1=0.1$,$k_3=0.09$,k_2 均在(k_3,k_1)取值。

在优选交叉操作之后进行变异操作。为保证算法能够做到全局收敛,本文采用了非均匀变异方法[9]。假设 $V=(v_1,v_2,\cdots,v_k,\cdots,v_n)$为原染色体,$V'=(v_1,v_2,\cdots,v_k',\cdots,v_n)$为经过非均匀变异后的新染色体,同时假设变异点 v_k 处的取值区间为$[U_{\min}^k,U_{\max}^k]$,则变异点处的新基因值 v_k'的计算公式为:

$$v_k'=\begin{cases}v_k+(U_{\max}^k-v_k)\cdot(1-r^{(1-t/T)b}),r\leqslant 0.5\\ v_k-(v_k-U_{\min}^k)\cdot(1-r^{(1-t/T)b}),r>0.5\end{cases} \tag{8}$$

其中,t 表示种群的总进化代数,r 表示在[0,1]内非均匀分布的随机数,T 表示最大的进化代数,b 表示系统参数(通常设为 2)。

3 算法流程设计

在对神经网络进化算法的改进中,在交叉概率算子和变异概率算子的计算中采用了个体适应度概率方差,这样能提高遗传算法的收敛速度。同时,引入模拟退火算法对交叉子代进行取舍,也加

快了遗传迭代的进度。基于前文对神经网络进化算法的改进并参考文献[11],设计 AENNA 的实现步骤如下:

步骤 1 设定初始参数。设置 BP 神经网络的层数、每层神经元个数、样本数据模式和误差值等。

步骤 2 初始化操作。用符合正态分布的小随机数随机产生 p 个染色体 bi 作为初始化的大种群。

步骤 3 估算操作。根据权值、阈值向量,用 BP 算法处理输入、输出样本,获得全局误差 E。若 E 满足条件,则结束,若个体适应度值符合设定要求,则结束;否则转入步骤 4。

步骤 4 小种群演化操作(小种群的演化操作流程如图 1 所示)。将大种群中的个体按照编码长度的差异重组为多个小种群,并对每个小种群进行 m 代的进化处理。

步骤 4.1 选择操作。按式(3)和式(4)的选取概率,采用高适应度值、高概率选择法从父代中选择个体进行计算。

步骤 4.2 交叉操作。按式(1)计算交叉概率,并依据式(5)和式(6)进行交叉运算。

步骤 4.3 对交叉后的个体进行模拟退火处理,做出必要的取舍。

步骤 4.4 变异操作。按式(7)计算变异概率,并依据式(8)进行变异运算。

步骤 4.5 判断操作。若进化代数 $G<m$,则从每个小种群中挑选优秀个体,并计算其适应度值,若满足条件,则算法结束;否则,重复步骤 4.1~步骤 4.4 的操作;若进化代数 G 达到 m,则选取一个优秀个体返回大种群中,以代替小种群,并转至步骤 5 继续运算。

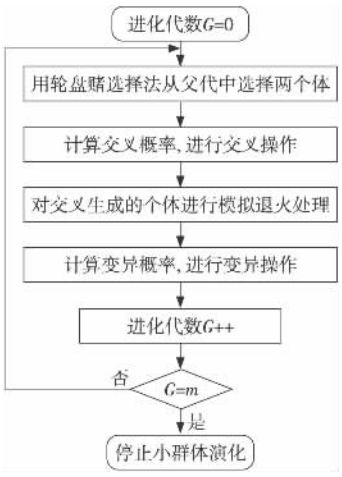

Figure 1 Small population evolution process

图 1 小种群演化操作流程

步骤 5 大种群演化(大种群演化操作流程如图 2 所示)。大种群中主要是不同结构网络的演化竞争,个体按式(3)和式(4)的选择概率计算公式进行改变其网络结构的演化运算,其变异算子步骤如下:

步骤 5.1 删除操作。将隐含层中所包含的某些节点的权值设置为 0,即删除节点及其连接。

步骤 5.2 增加操作。添加一些节点到隐含层,并产生相应的权值,然后按式(7)进行自适应变异。

步骤 6 新的大种群重组,转到步骤 3。

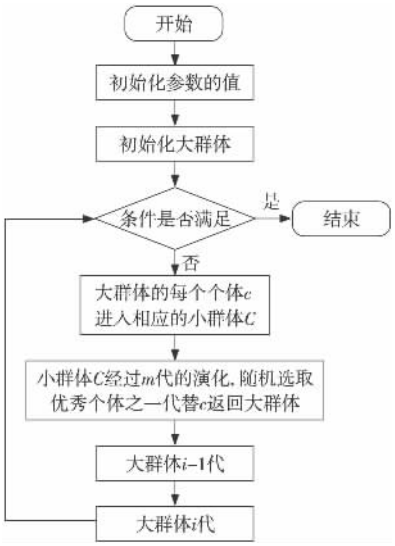

Figure 2 Big population evolution process

图 2 大种群演化操作流程

4 基于 AENNA 的入侵检测

基于 AENNA 算法的入侵检测系统模型如图 3 所示,其中包括数据捕获引擎、特征提取模块、数据预处理模块、数据库、AENNA 训练模块、AENNA 分类器模块和响应模块。

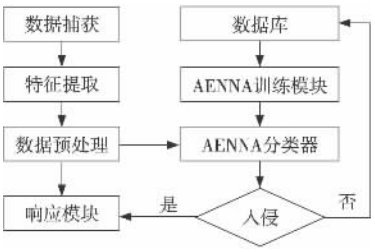

Figure 3 Intrusion detection model based on AENNA

图 3 基于 AENNA 的入侵检测模型

数据捕获引擎模块负责在网络中发送和接收数据包。特征提取模块主要将网络数据包信息转化为包含对应数据包特征值的网络连接记录。数

据预处理模块负责将字段数值归一化到一个较小的区间范围,减少由于记录间字段数值差异过大而引发的网络训练不良表现。数据库模块主要是为了方便存储,选用数据库存放预处理模块处理的数据以及通过分类器检测后的结果。AENNA 训练模块将从数据库中提取标准的数据(包括给定的样本记录向量和网络训练要达到的目标)对分类器进行训练。AENNA 分类器模块可以对输入中的未知的网络连接记录判别为正常或入侵,并做出相应处理。响应模块主要用以接收从 AENN 分类器检测出的结果,并对入侵行为发出警报。

本文的重点是设计对 AENNA 分类器,其原理是应用数据及划分后的训练样本集对 BP 神经网络分类器进行训练,在进化神经网络内部建立起对训练样本的识别模型并存储这些攻击行为的特征模式;然后对捕获的网络数据流进行分析处理,以区分正常的网络行为和异常网络行为;当检测到未知类型的攻击行为时,将其反馈给学习样本库以供 BP 神经网络进行再学习,从而体现 AENNA 算法分类引擎所具备的通过学习不断扩展检测范围的能力。

5 实验与结果分析

5.1 实验数据

目前入侵检测研究领域常用的数据集有 MIT LL、SOTM(Scan of the month)、Defcon 数据集及由哥伦比亚大学 IDS 实验室基于 MITLL 采集整理形成的 KDD CUP99 数据集。由于 MIT LL 数据集未经格式化处理,数据的攻击特征不规范;SOTM 和 Defcon 数据集中数据无攻击标记,数据筛选比较复杂繁琐;KDD CUP99(简称 KDD99)对 MIT LL 数据集的网络流量进行了格式化处理,改进并规范了特征的表示,提供了适用于各种入侵检测算法进行测试和评估的数据集[12]。所以,KDD99 网络数据集仍是目前公认的最优秀且影响最广泛的网络安全审计数据集,自公布以来出现了许多基于此数据集的研究成果和研究论文。因此,为了验证 AENNA 入侵检测算法的检测效果,本文采用 KDD99 数据集进行检测验证实验。

KDD99 数据集是入侵检测领域通用的实验数据集,其中包括四种攻击类型的 39 种不同攻击的大约 500 万条连接记录,22 种出现在训练数据集中,17 种出现在测试集中。四种类型分别是刺探攻击 Probe、拒绝服务 DOS、获取根权限 U2R、远程攻击 R2L。

原始数据集中记录数过于庞大,依据各类型所占比例,从 KDD data_10_percent 和 Correct 中提取相应的攻击记录,其中 DOS 攻击记录约占 94%,Probe 攻击记录数约占 3%,R2L 攻击记录数约占 2%,U2R 攻击记录数约占 1%。在攻击集的基础上,选取一部分正常连接记录数据与 DOS 数据记录,按照 1∶3 的概率将其混杂入正常数据流量集,形成不均衡数据集。选取 49 400 个有效数据形成训练集,并选取 80 500 个数据构成测试集[12]。

数据集中每个网络连接记录中都包含 41 维数据,利用信息熵理论[13],计算数据集中每个特征判定网络连接为攻击还是正常状态的信息量,并按信息量大小进行排列,最终选取判定所含信息量较大的前 10 维特征用于实验,从而实现数据集中连接记录特征的降维,形成了更为高效精简的数据集以用于后续的实验。实验数据的具体构成如表 1 所示。

Table 1 Composition of experimental data sets

表 1 实验数据集的组成

数据集名称	训练样本数据集	测试样本数据集
DOS 样本数	33 793	54 537
Probe 样本数	377	591
U2R 样本数	6	20
R2L 样本数	62	112
异常样本数	34 238	55 260
正常样本数	15 162	25 240
总样本数	49 400	80 500

5.2 实验测试与结果

实验测试环境为 PC 机,操作系统为 Windows XP、奔腾双核 2.0 GHz CPU、2 GB 内存,采用 Matlab 7.0 结合 Myeclipse 8.5 软件平台在 PC 机上对 AENNA 算法进行仿真实现,并利用已实现的算法仿真模块对表 1 中的 KDD 实验数据集进行检测验证实验。

首先采用 AENNA 算法结合实验训练数据集对 BP 神经网络进行训练,并将训练好的神经网络用于入侵检测,利用实验测试数据集测试其检测性能;其次与将 BP 神经网络算法、遗传算法、传统进化神经网络算法作为训练算法的训练好的神经网络的检测性能做对比。

为了更容易观察和调整 BP 神经网络的训练结果,根据实际情况,本文采用仅含有一个隐含层

的 BP 神经网络。根据 2.1 节中算法的改进思路，利用大小双种群来优化进化神经网络的隐层节点数，从而确定网络结构。由于 Sigmoid 函数是一个连续可微的函数，可以将输入值映射到[0,1]内，方便进化神经网络的处理，可以满足 BP 模型对传递函数的连续可微的要求，因此将其作为传递函数。初始权值则通过随机的方法将其置为－10～10 的小随机数。其余的网络权值及阈值则通过改进的自适应进化算法来进行优化。

根据上述规则设定参数，并参考文献[11]，在对 AENNA 的仿真实现中，网络权值取值区间定义为(－10,10)，将精确度确定为 0.01，设置输入节点个数为 10，输出节点数为 2，误差精度设为±0.01，并设置不同的种群、隐含层节点、进化代数的参数进行对比实验，实验结果如表 2 所示。

Table 2 Comparison of experimental results under different parameters

表 2 不同参数取值的实验结果比较

种群大小	隐层节点数	种群的进化代数	最好个体适应度值
140	6	70	0.9906
155	7	90	0.9950
200	8	120	0.9929

由表 2 可见，当隐含层的节点数为 7 时，AENNA 中个体的适应度在较小的遗传代数后取得最优值。因此，优化后的网络结构为“10-7-2”。将网络权值和阈值作为优化结构后的 BP 神经网络的初始权值和阈值，输入实验训练样本数据集对其进行训练。样本训练完成后，利用 KDD 实验测试数据集在已知 BP 神经网络上进行入侵检测测试，得到的检测结果如表 3 所示。

Table 3 Intrusion detection results based on AENNA

表 3 基于 AENNA 的入侵检测结果

检测指标	检测结果
检测率	0.9879
误报率	0.0015
漏报率	0.0023

由表 2 和表 3 可见，在入侵检测实验中，当种群大小设定为 155 个、隐含层节点数设定为 7 层且进化代数设为 90 次时，基于 AENNA 的入侵检测效果最佳，此时的误报率和漏报率都相对较小。

为进行训练算法的检测性能对比，根据参考文献[11]中的参数设置，特设定统一的实验参数值，如表 4 所示。

采用实验中的精简数据集，对 BP 神经网络算法、遗传算法、传统神经网络进化算法和基于 AENNA 的入侵检测方法进行检测对比，其中 BP 神经网络的输入节点数为 10，输出节点数为 2，隐含层节点设为 6，遗传算法的初始种群设为 50，适应度函数采用基于误差函数的适应度函数。检测效果对比如表 5 所示。

Table 4 Parameters setting of comparison test

表 4 对比实验的参数设置

参数指标	参数值	参数指标	参数值
训练最大次数	1000	杂交概率	0.8
误差	0.0001	变异概率	0.01
学习率	0.01	遗传代数	200
初始权值	[－1.0,1.0]		

Table 5 Comparison of intrusion detection performance

表 5 入侵检测效果比较

	BP 神经网络算法	遗传算法	传统神经网络进化算法	AENNA
已知行为检测率	0.9489	0.9579	0.9641	0.9879
未知行为检测率	0.8223	0.8472	0.8919	0.9049
误报率	0.0399	0.0390	0.0089	0.0015

从表 5 中可以清楚地看出，基于 AENNA 的入侵检测算法不但对已知入侵行为有较高的检测率，而且对于未知入侵行为也有较好的检测率。与采用 BP 算法、遗传算法和进化 BP 算法的入侵检测方法相比，AENNA 的入侵检测算法有较高的检测率和较低的误报率。

6 结束语

为提高入侵检测系统的检测效率，本文在进化神经网络算法基础上，提出一种自适应进化神经网络算法(AENNA)，以大小两个种群的双种群遗传策略为着眼点，通过改进交叉算子和变异算子的计算方式及公式参数，结合模拟退火算法对遗传算法进行了改进，并利用遗传算法对 BP 神经网络算法进行网络结构及连接权值优化。通过与其他主流入侵检测算法的检测性能对比实验，表明基于 AENNA 的入侵检测算法对入侵检测系统的检测性能有较大的提升。由于在遗传算法的改进中引入了模拟退火算法思想，增加了整个算法的时间复杂度，因此下一步研究将解决时间复杂度过高的问题。

参考文献：

[1] Qing Si-han, Jiang Jian-chun, Ma Heng-tai, et al. Research

on intrusion detection techniques: A survey[J]. Journal of China Institute of Communications, 2004, 25(7):19-29. (in Chinese)

[2] Wang Qi-an, Chen Bing. Intrusion detection system using CVM algorithm with extensive kernel methods[J]. Journal of Computer Research and Development, 2012, 49(5):974-982. (in Chinese)

[3] Wang Tao. Association decision based multiple source network intrusion detection algorithm[J]. Computer Simulation, 2012, 29 (8):120-122. (in Chinese)

[4] Gong Xing-chao, Guan Xin. Intrusion detection model based on the improved neural network and expert system[C]// Proc of IEEE Symposium on Electrical & Electronics Engineering, 2012:191-193.

[5] Srinivas M, Andrew H. A comparative study of techniques for intrusion detection[C]// Proc of the 23rd IEEE International Conference on Tools with Artificial Intelligence, 2009: 570-577.

[6] Ren Zi-wu, San Ye. Improved adaptive genetic algorithm and its application research in parameter identification[J]. Journal of System Simulation, 2006, 18(1):41-66. (in Chinese)

[7] Huang Li-jun, Xu Yong-hua. Solving TSP converged on genetic algorithm and the ant algorithm[J]. Journal of Northeast Agricultural University, 2008, 39(4):109-113. (in Chinese)

[8] Li Shu-hui, Ma Li, Xu Xue-zhou. Intrusion detection techniques research based on genetic neural networks [J]. Modern Electronic Technique, 2005(5):78-80. (in Chinese)

[9] Yan Yan. A new adaptive genetic algorithm[D]. Harbin: Harbin Engineering University, 2007. (in Chinese)

[10] Yang Wei-bo, Zhao Yan-wei. Improved simulated annealing algorithm for TSP [J]. Computer Engineering and Applications, 2010, 46(15):34-36. (in Chinese)

[11] Li Shu-hui. Improved evolutionary neural network algorithm and its applications in intrusion detection[J]. Modern Electronic Technique, 2010, 33(1):78-80. (in Chinese)

[12] Zhang Xin-you, Zeng Hua-can, Jia Lei. Research of intrusion detection system dataset-KDD CUP99[J]. Computer Engineering & Design, 2010, 31(2):4809-4813. (in Chinese)

[13] Xu Yong-hua, Li Guang-shui. Incremental SVM intrusion detection algorithm based on distance weighted template reduction and attribute information entropyc [J]. Computer Science, 2012, 39(12):76-78. (in Chinese)

附中文参考文献:

[1] 卿斯汉, 蒋建春, 马恒太, 等. 入侵检测技术研究综述[J]. 通信学报, 2004, 25(7):19-29.

[2] 王奇安, 陈兵. 基于广泛内核的 CVM 算法的入侵检测[J]. 计算机研究与发展, 2012, 49(5):974-982.

[3] 王涛. 基于关联决策算法的网络多源入侵检测[J]. 计算机仿真, 2012, 29(8):120-122.

[6] 任子武, 伞冶. 自适应遗传算法的改进及在系统辨识中应用研究[J]. 系统仿真学报, 2006, 18(1):41-66.

[7] 黄立君, 许永花. 遗传算法和蚁群算法融合求解 TSP[J]. 东北农业大学学报, 2008, 39(4):109-113.

[8] 李淑慧, 马力, 徐学洲. 基于遗传神经网络的入侵检测方法研究[J]. 现代电子技术, 2005(5):78-80.

[9] 闫妍. 一种新的自适应遗传算法[D]. 哈尔滨: 哈尔滨工业大学, 2007.

[10] 杨卫波, 赵燕伟. 求解 TSP 问题的改进模拟退火算法[J]. 计算机工程与应用, 2010, 46(15):34-36.

[11] 李淑慧. 改进进化神经网络算法及其在入侵检测中的应用[J]. 现代电子技术, 2010, 33(1):78-80.

[12] 张新有, 曾华燊, 贾磊. 入侵检测数据集 KDD CUP99 研究[J]. 计算机工程与设计, 2010, 31(2):4809-4813.

[13] 徐永华, 李广水. 基于距离加权模板约简和属性信息熵的增量 SVM 入侵检测算法[J]. 计算机科学, 2012, 39(12): 76-78.

作者简介:

杨宏宇(1969-),男,吉林长春人,博士后,教授,研究方向为网络信息安全。**E-mail**: yhyxlx@hotmail.com

YANG Hong-yu, born in 1969, post doctor, his research interest includes network information security.

赵明瑞(1985-),男,河北衡水人,硕士生,研究方向为网络信息安全。**E-mail**: Zhaomingrui545@163.com

ZHAO Ming-rui, born in 1985, MS candidate, his research interest includes network information security.