# 一种改进 QPSO 优化 BP 网络的入侵检测算法

何伟山,秦亮曦
(广西大学 计算机与电子信息学院,广西 南宁 530004)

**摘 要**:为了较好克服量子粒子群算法存在早熟收敛的缺点,在分析算法参数和流程的基础上,提出了一种带变异操作的改进量子粒子群优化算法。针对传统 BP 算法易于陷入局部极小的不足,将改进的算法应用到 BP 神经网络的学习过程中,修正 BP 网络的权值和阈值,提高其收敛性能。并将优化的 BP 神经网络模型应用于入侵检测中,用标准入侵检测数据对基于不同算法的 BP 网络进行仿真实验比较。实验结果表明,改进后的 BP 算法迭代次数少,收敛速度有所提高,在一定程度上提高了入侵检测率。

**关键词**:入侵检测;BP 神经网络;量子粒子群优化;变异操作;自适应变异量子粒子群
**中图分类号**:TP301.6 **文献标识码**:A **文章编号**:1673-629X(2013)12-0147-04
doi:10.3969/j.issn.1673-629X.2013.12.035

# An Intrusion Detection Algorithm of BP Network Optimized by Improved QPSO

HE Wei-shan, QIN Liang-xi
(School of Computer and Electronics and Information, Guangxi University, Nanning 530004, China)

**Abstract**: In order to overcome the shortcomings of the quantum particle swarm optimization algorithm better, which is precocious convergence, on the basis of analyzing algorithm parameters and processes, an improved quantum particle swarm optimization algorithm with mutation operation has been proposed. Because the traditional BP algorithm is easy to fall into local minima, the improved algorithm is applied in the learning process of the BP neural network to correct weights and threshold of BP network, and improve the convergence performance. The optimized BP neural network is used in the intrusion detection, and simulation experiments on BP network with different algorithm is made with standard intrusion detection data. The results show that the improved BP algorithm has less number of iterations, the convergence rate has increased, improving the intrusion detection rate too.

**Key words**: intrusion detection; BP neural network; quantum particle swarm optimization; mutation operation; adaptive mutation quantum particle swarm

## 0 引 言

随着网络技术的发展,网络信息安全问题日益突出,已经严重威胁到人们的正常生活,因此计算机系统和网络安全防护技术越来越受到人们的重视。针对这些信息安全问题,采取了一些防护措施,最常见的手段有信息加密技术、身份安全认证、防火墙等技术,这些都是静态和被动的防御方式,不可避免地存在一些漏洞,而入侵检测作为一种主动积极的安全防御技术有效弥补了某些方面的不足。

传统的入侵检测方法,主要集中在量化分析和数据统计方面,存在检测精度不高、检测方法单一等问题。因此,神经网络、遗传算法、免疫学、SVM 等智能方法逐渐应用到入侵检测算法。文献[1-2]最早分析了 BP 神经网络具有非线性、自组织和自学习等一些特性,应用在模式识别和入侵检测中十分有效。而传统 BP 算法是一种梯度下降学习法,训练大样本集时存在学习速度较慢、易陷入局部极小等问题。文献[3-4]分别提出了用遗传算法、粒子群优化算法优化 BP 网络的方法,取得了一定的效果。文献[5-6]中提出了具有量子行为的粒子群优化算法,与标准粒子群算法相比,具有较好的全局搜索性能。

虽然说量子粒子群算法具有较好的全局搜索能力,但是在迭代进化过程中,由于缺少交叉、变异等遗

**收稿日期**:2013-03-08 **修回日期**:2013-06-15 **网络出版时间**:2013-09-29
**基金项目**:"十一五"国家科技支撑计划课题(2009BAH53B03)
**作者简介**:何伟山(1985-),男,湖北大悟人,硕士研究生,研究方向为人工智能、数据挖掘;秦亮曦,教授,研究方向为数据挖掘、进化计算。
**网络出版地址**:http://www.cnki.net/kcms/detail/61.1450.TP.20130929.1544.042.html

传操作,不可避免地减少了群体的多样性,也存在早熟收敛的问题。针对量子粒子群优化算法由于种群多样化减少而存在早熟收敛的问题,文中提出了一种带变异操作的量子粒子群优化算法(MQPSO),用改进算法优化 BP 网络的学习,并把改进的 BP 网络模型应用于入侵检测中。通过 KDD99 CUP 数据集分别对三种不同的 BP 学习算法进行了仿真实验比较,结果表明优化的 BP 算法收敛速度较快,在一定程度上避免了早熟收敛,提高入侵检测的准确率,有效降低误报率。

## 1 入侵检测的概念及原理

常见入侵活动主要包括未经授权用户非法存取数据、修改数据或者破坏计算机的正常运行等,这些入侵行为企图破坏计算机系统或网络的机密性、完整性以及可用性。入侵检测[7](Intrusion Detection)就是对企图入侵或已经入侵的行为进行识别和分析处理的过程。入侵检测系统(Intrusion Detection System)是收集和检测计算机系统或网络中入侵信息并做出反应,从而发现是否有违反安全策略行为的一种主动防御技术。

入侵检测是一种动态的安全防护手段,在不影响网络性能的前提下,对各种非法入侵行为进行识别,对系统和网络中未授权的访问或异常活动进行追踪、审计、识别、检测和处理。入侵检测系统主要包括信息收集、数据分析和结果处理 3 个基本过程,如图 1 所示。其主要工作原理是:从系统不同节点收集信息并分析该信息,寻找入侵活动的特征行为,并主动对检测到的行为做出响应,最终记录检测过程并报告检测结果。

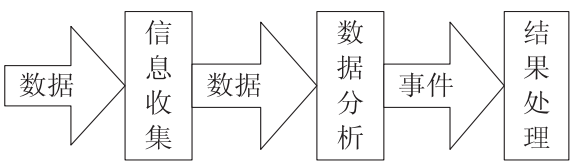


图 1 入侵检测过程

## 2 BP 神经网络

BP 神经网络是典型的前馈网络,结构上它属于多层前向网络。它分为输入层、隐层和输出层,各层之间互相连接,每一层权值可以通过学习来调节。BP 网络不仅含有输入节点和输出节点,而且含有一层或多层隐节点,节点的激励函数通常采用典型函数 S 表示[8]:

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

其中 $x$ 是神经元的加权输入函数。BP 网络的学习过程中,首先输入所用的学习样本集,通过确定的网络结构和前一次迭代的权值和阈值,从 BP 网络的第一层向后计算每个神经元的输出;然后对权值和阈值进行修改,从最后一层向前计算各权值和阈值对总误差的影响,进而对各权值和阈值进行修改。这两个步骤交替进行,误差会逐层往回传递,进一步修正层与层间的权值和阈值,直到出现收敛为止。

## 3 改进量子粒子群算法优化 BP 网络

### 3.1 量子粒子群算法

2004 年,Jun Sun 等人在粒子群优化算法(PSO)的基础上,将量子进化观点引入到粒子群算法中,提出了量子粒子群优化算法(QPSO)模型[3-4]。量子粒子群算法以 DELTA 趋阱为基础,认为每个粒子具有量子行为,因此具有量子行为的粒子在移动时并没有确定的轨迹,可以在全部可行解空间中进行探索,以便得到全局最优解。这样的模型使得 QPSO 算法比标准 PSO 算法具有更优的全局搜索能力。在 QPSO 算法中,设种群规模为 $M$,公式变换为:

$$P = aP_{\text{best}}(i) + (1 - a) \times G_{\text{best}},$$
$$m_{\text{best}} = \frac{1}{M}\sum_{i=1}^{M} P_{\text{best}}(i) \tag{2}$$

$$b = 1.0 - \text{generation}/\text{max generation} \times 0.5 \tag{3}$$

$$\text{position} = p \pm b \times |m_{\text{best}} - \text{position}| \times \ln(1/u) \tag{4}$$

其中,$m_{\text{best}}$是粒子群极值 $P_{\text{best}}$的中间位置,即平均值;generation 为当前进化代数;max generation 为设定的最大进化代数;$a$、$u$ 为[0,1]之间的随机数;$b$ 为收缩扩张系数。可以看出,QPSO 和 PSO 的不同点在于更新粒子位置的方法不同。在 PSO 算法中,粒子必须在一个有限的搜索范围内以确保粒子群的聚集性,从而使算法收敛于全局最优点或局部最优点。QPSO 算法与 PSO 相比,粒子能够以某一确定的概率出现在整个可行搜索空间中任意一个位置,而此位置可能比当前群体中 $P_{\text{best}}$ 具有更好的适应度值。因而 QPSO 具有调节参数少、简单易实现的优点,具有良好的收敛性和全局搜索能力。

### 3.2 量子粒子群算法改进

虽然 QPSO 具有算法简单易行和收敛速度快等优点,但由于降低了粒子的多样性,搜索后期粒子聚集,搜索空间十分有限,可能陷入局部极值。为了增强算法的全局寻优能力,避免算法收敛于局部最优,文中尝试在量子粒子群优化算法中引入变异机制,对全局极值进行变异操作,以增加种群多样性,这样更易于找到全局最优解。要判别算法收敛过程,根据量子粒子群算法的粒子行为特征,无论是早熟收敛还是全局收敛,粒子都呈现出聚集现象,根据种群中所有个体的适应度的整体变化可以跟踪粒子的状态,作为早熟收敛判

断的主要条件[9]。

设粒子群的粒子数目为 $n$,$f_i$ 为第 $i$ 个粒子的适应度,$f_{avg}$ 为粒子群目前的平均适应度,$\sigma^2$ 为粒子群的群体适应度方差,则可定义为:

$$\sigma^2 = \sum_{i=1}^{n} \left| \frac{f_i - f_{avg}}{f} \right|^2 \tag{5}$$

其中,$f$ 作用是限制 $\sigma^2$ 的大小,该算法中 $f$ 的取值采取如下公式:

$$f = \begin{cases} \max_{1 \leqslant i \leqslant n} |f_i - f_{avg}|, \max |f_i - f_{avg}| > 1 \\ 1, \text{else} \end{cases} \tag{6}$$

从上面的公式可以看出,种群适应度方差反映了粒子群所有粒子的聚集程度,方差越小粒子的聚集程度越大。随着迭代次数的增加,种群个体的适应度会越来越接近,因此方差会越来越小,如果粒子群算法优化算法陷入早熟收敛,群体适应度方差趋向于零,而空间位置聚集度越小时陷入局部收敛,故当 $\sigma^2 < C$ ( $C$ 为给定阈值)时,认为进入后期搜索,出现早熟收敛现象。

为了实现变异操作,构造变异概率 $P_m$,表示为:

$$P_m = \begin{cases} \exp(-h)/5.0, \sigma^2 < \sigma_1 \\ 0, \quad \sigma^2 \geqslant \sigma_1 \end{cases} \tag{7}$$

其中,适应度方差 $\sigma^2$ 由公式(5)决定;$\sigma_1$ 是给定的阈值,一般趋近于 0;$h$ 是空间位置聚集度。根据构造变异概率对部分粒子进行变异,使粒子分散开来。产生随机数 $r \in [0,1]$,如果 $r < P_m$,对每个极值进行一个扰动,根据 $p_i = p_i(1 + 0.5\eta)$ 来决定,$p_i$ 是第 $i$ 个粒子目前最好的位置,$\eta$ 是服从(0,1) 正态分布的 $n$ 维随机向量。

### 3.3　改进量子粒子群优化算法的实现

从上面的分析可以看出,在带变异操作的 QPSO 算法的参数中,变异概率 $P_m$ 的选择是影响算法性能的关键。选择合适的变异概率对全局极值 $G_{best}$ 进行变异操作,这样增加了粒子位置的多样性,也改变了粒子的前进方向,进而可以让粒子进入搜索空间中的其他位置进行搜索,使算法发现新的个体极值 $P_{best}$ 以及 $G_{best}$,如此反复的迭代,算法能更好地找到全局最优解。

改进的 MQPSO 算法的具体描述如下:

步骤 1:初始化粒子群各参数,包括个体极值 $P_{best}$ 和全局极值 $G_{best}$ 等,确定种群规模和粒子维数。

步骤 2:根据目标函数计算各个粒子的适应度值,判断收敛准则是否满足,如果满足转步骤 7,否则继续执行步骤 3。

步骤 3:根据适应度,更新当前个体最优位置和种群最优位置,生成新的粒子群。

步骤 4:每个粒子比较它的适应度值和全局极值,如果它的适应度值更好,则更新当前的全局极值。

步骤 5:计算粒子的适应度方差 $\sigma^2$,根据式(7)计算变异概率。

步骤 6:产生随机数 $r$,如果 $r < P_m$,则执行变异操作,否则转向步骤 7。

步骤 7:判断粒子适应度是否满足收敛条件或者是否达到进化最大代数,是则退出,否则返回步骤 2。

步骤 8:置 $t = t + 1$,转步骤 2。

步骤 9:输出全局极值 $G_{best}$ 及其适应值。

### 3.4　基于改进算法的 BP 网络

由于传统 BP 算法存在收敛速度慢、容易陷入局部极小的缺点,文中将改进的 MQPSO 算法引入到 BP 网络学习训练中,优化 BP 网络的权值和阈值,避免 BP 神经网络自身存在的局部收敛性问题,提高 BP 神经网络的训练精度。BP 神经网络应用于入侵检测是一种十分有效的方法,它可以通过大量实例运用训练的方法学习与获取知识,并获得一定的预测能力,通过再训练可以使神经网络的攻击模式产生变化,从而发现新的入侵攻击实例,这样使得入侵检测系统具有自适应能力[10]。

MQPSO 算法训练 BP 网络时,首先将神经网络结构中所有神经元之间的连接权值编码成实数串表示的个体,假设网络中包含 $N$ 个优化权值(包括阈值),则每个个体将由 $N$ 个权值参数组成的一个 $N$ 维向量来表示。然后按照个体结构随机产生一定数目的粒子组成种群,初始化两个最优值 $P_{best}$ 和 $G_{best}$,不同的个体代表神经网络的一组不同权值,对每一个体对应的神经网络,输入训练样本进行训练。经过 MQPSO 算法找到最优粒子,然后把最优粒子分解映射为 BP 网络的权值和阈值,进一步进行 BP 网络的学习训练,使 BP 网络最终达到最佳状态。可以看出网络权值的优化过程其实是一个反复迭代的过程。

## 4　仿真实验与总结

### 4.1　实验参数设计

为了验证提出的改进算法训练 BP 网络方法的有效性,文中采用标准入侵数据集采集样本 KDD99 CUP 数据集作为实验数据[11]。该数据集共有近 500 万条数据样本,每个样本包含了 41 个特征属性,数据集除正常连接 Normal 外还包含 24 种攻击,可以分为 Dos 拒绝服务、U2R 获取根权限、R2L 远程攻击、Probe 刺探攻击 4 种攻击类型。

仿真实验中,根据 BP 神经网络特性,只要隐层有足够单元可用,选用 3 层 BP 神经网络就可以完成任意的 $n$ 维到 $m$ 维的映射[12],设 BP 网络为 3 层,输入和输出向量的维数确定输入和输出层的神经元数目。实

验中选用 41 个特征数据作为输入数据,目标数据为一维实数向量,所以输入层神经元个数为 41,输出层神经元个数为 1。

学习算法 MQPSO 初始参数设置,种群规模 $n=30$,学习因子 $c_1$ 和 $c_2$ 最大速度 = 2,惯性权重 $W=0.8$,最大迭代次数为 500。

### 4.2 仿真结果分析

该实验数据样本从 KDD99 CUP 数据集中随机抽取 6 000 条记录,其中训练集样本 2 300 条记录,测试集为 3 700 条记录,样本集分别分为 Normal、Dos、U2R、R2L 和 Probe 五种攻击类型进行测试,最终与基于 QPSO 算法和 MPSO 算法的 BP 神经网络做仿真实验比较。

最终的仿真实验结果和比较如图 2 和表 1 所示。图 2 的仿真结果表明,改进的带变异操作的量子粒子群算法(MQPSO)分别与 MPSO 和 QPSO 算法优化的 BP 网络相比,在进化迭代次数相同的条件下,改进的 MQPSO 算法收敛速度较快,算法性能有明显提高。

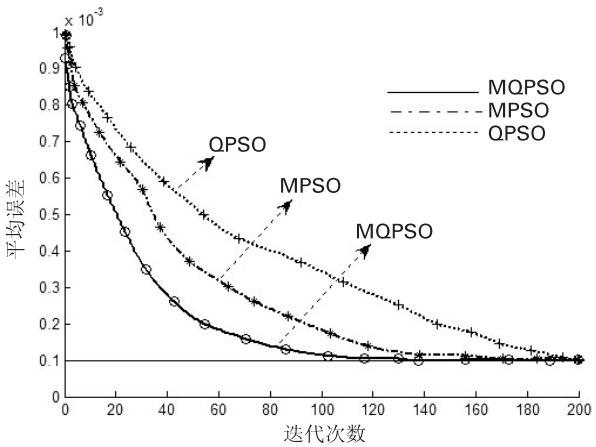


图 2 仿真实验结果

表 1 检测结果比较

| 攻击类型 | QPSO | | MPSO | | MQPSO | |
|---|---|---|---|---|---|---|
| | 检测率/% | 误报率/% | 检测率/% | 误报率/% | 检测率/% | 误报率/% |
| Normal | 90.2 | 1.98 | 93.1 | 1.73 | 95.8 | 1.62 |
| Dos | 91.3 | 2.03 | 94.7 | 1.95 | 96.2 | 1.59 |
| U2R | 95.4 | 0.92 | 96.1 | 0.85 | 97.0 | 0.69 |
| R2L | 93.9 | 0.93 | 95.6 | 0.73 | 98.1 | 0.46 |
| Probe | 95.7 | 1.89 | 96.4 | 1.65 | 98.3 | 1.26 |

表 1 的实验结果说明,MQPSO 训练的 BP 算法应用在入侵检测中,检测率有所提高,也降低了误报率。因此改进的带变异操作的量子粒子群算法优化的 BP 网络应用于入侵检测,其收敛速度和算法性能与一般的 QPSO 算法和 MPSO 算法相比都有所改善。

## 5 结束语

文中针对传统的 BP 算法和量子粒子群优化算法存在容易陷入局部最优和易于早熟收敛的不足,提出了一种带变异操作的改进量子粒群优化算法,避免因种群减少而早熟收敛的缺点,并将基于改进算法的 BP 神经网络模型应用于入侵检测中,与几种不同的 BP 算法进行了仿真实验比较。实验结果表明:改进的 MQPSO 算法优化 BP 网络迭代次数较少、收敛速度快,而且入侵检测的准确率也有一定提高。在今后的研究工作中,针对 BP 神经网络自身存在的缺陷,尝试使用更多改进智能算法对 BP 网络进行优化,以便得到更好的效果,因此将改进的 BP 网络应用于入侵检测,具有一定的实际应用效果和较好的研究价值,值得进一步深入探讨。

**参考文献:**

[1] Tan K. The application of neural network to UNIX computer security[M]. [s. l. ]:Addison-Wesley,1992.

[2] Jake R, Meng Jianglin. Intrusion detection with neural networks[C]//Proc of the 13th national computer security conf. [s. l. ]:[s. n. ],1998:86-90.

[3] 徐仙伟,叶小岭. 遗传算法优化 BP 网络初始权重用于入侵检测[J]. 计算机应用研究,2005,22(3):127-128.

[4] 肖晓丽,黄继红,刘志朋. 基于 MPSO 的 BP 网络及其在入侵检测中的应用[J]. 计算机工程,2008,34(15):168-169.

[5] Sun Jan,Xu Wenbo. A global search strategy of quantum-behaved particle swarm optimization[C]//Proceedings of IEEE conference on cybemetics and intelligent systems. Wuxu:[s. n. ],2004:111-116.

[6] Sun Jan, Feng Bin, Xu Wenbo. Particle swarm optimization with particles having quantum behavior[C]//Proceedings of 2004 congress on evolutionary computation. Wuxu:[s. n. ], 2004:325-331.

[7] Sherif J S. Intrusion detection:System and models[C]//Proceedings of the eleventh IEEE international workshops on enabling technologies:Infrastructure for collaborative enterprises. California:[s. n. ],2002.

[8] 黄高隽. 人工神经网络原理及仿真实例[M]. 北京:机械工业出版社,2003.

[9] 孙 勇,章卫国,章 萌,等. 基于改进粒子群算法的飞行控制器参数寻优[J]. 系统仿真学报,2010,22(5):1222-1225.

[10] Shun J,Malki H A. Network intrusion detection system using neural networks[C]//Proc of fourth international conference on natural computation. Jinan:[s. n. ],2008:242-246.

[11] 陈晓梅. 入侵检测中的数据预处理问题研究[J]. 计算机科学,2006,33(1):81-83.

[12] 田雨波. 混合神经网络技术[M]. 北京:科学出版社,2009.

# 一种改进QPSO优化BP网络的入侵检测算法

作者： 何伟山， 秦亮曦， HE Wei-shan， QIN Liang-xi
作者单位： 广西大学 计算机与电子信息学院,广西 南宁,530004
刊名： 计算机技术与发展
ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2013(12)