粒子群 BP 神经网络在 DDoS 攻击检测中的应用*

李 锋
(广东交通职业技术学院,广东 广州 510650)

摘 要：利用 BP 神经网络自适应学习，结合粒子群优化算法的全局搜索和遗传算法的快速收敛特性检测 DDoS 攻击行为。实验证明,新算法具有速度快、检测率高和误报率低的特点,能很好地应用于检测和抵御 DDoS 攻击。

关键词：DDoS;BP 神经网络;粒子群算法;遗传算法
中图分类号：TP391 **文献标识码**：A **文章编号**：1674-7720(2014)03-0050-05

Application of particle swarm BP neural network in DDoS attack detection

Li Feng
(Guangdong Communication Polytechnic, Guangzhou 510650, China)

Abstract: This paper uses BP network's learning and adaptive feature, combined with PSO algorithm's overall search and genetic algorithm's rapid convergence to detect DDoS attack. Experimental shows that the new algorithm has fast speed, high detection rate and low miss report rate, which can be applied to detect DDoS attacks.

Key words: DDoS; BP neural network; PSO algorithm; genetic algorithm

DDoS 是一种分布式大规模流量攻击方式，通过控制互联网上傀儡机对目标服务器发动攻击，产生的大量数据流涌向目标服务器，消耗服务器系统资源和带宽，或把链接占满，从而影响合法用户的访问。实施 DDoS 攻击一般都会伪造源 IP 地址，具有隐蔽性强、并发数高、攻击流量大、破坏力强、涉及范围广的特点。传统的 DDoS 检测方法很难界定突发流量与 DDoS 攻击流量。本文提出一种基于粒子群 BP 神经网络的流量检测模型，结合粒子群算法的全局搜索和遗传算法的快速收敛特性检测 DDoS 攻击行为，最后通过实验证明，新算法能够快速、准确地检测到各类 DDoS 攻击，具有很强的应用价值。

1 DDos 攻击方式和检测方法

DDoS 攻击基于 TCP 3 次握手协议，按攻击方式分为直接型攻击和反射式攻击两类。直接型攻击是通过控制傀儡机向目标服务器发送大量数据流，耗尽服务器系统资源直至瘫痪。反射式攻击是伪造服务器 IP 向主机群发送虚假连接请求，致使主机群应答信息涌向服务器(如 DNS 请求只有 60 B，应答信息却有 4 320 B，反射 70 多倍流量)，通过占尽服务器接入带宽和连接上限阻止合法用户的访问。

针对 DDoS 攻击通常采用的是基于特征库匹配检测、基于数据挖掘攻击检测和蜜罐技术[1]。特征库匹配检测需要搜集 DDoS 攻击数据包各种特征建立特征库，服务器对虚假连接请求特征进行匹配，若吻合则视为攻击。这种检测方法依赖于攻击特征的描述，对检测漏洞型 DDoS 很有效，但无法识别大量没有协议特征的攻击。基于数据挖掘攻击检测方法通过对数据包流量特征分析，将其中规律转换为检测规则，再根据网络流量特征是否偏离正常流量模型来判断攻击行为，其最大优点是能够检测没有协议特征的变种 DDoS 攻击，但是流量样本本身具有一定的随机性，使得算法复杂，计算量大，挖掘速率和准确性不高。蜜罐原本是一种网络诱骗技术，通过伪装真实系统特征吸引攻击者攻击蜜罐系统，而真正的服务器得以正常运行。蜜罐不能控制和阻断攻击行为，只有遭受攻击后才能检测到攻击，属于被动防御。上

*基金项目：2012 年广东省高等学校教学质量与教学改革工程省级精品资源共享课程(粤教高函[2013]13 号)；2013 年广东省高职教育教学指导委员会教学教改项目(xxjs-2013-2001)；2013 年广东省高职高专校长联席会议教改项目(GDXLHQN012)

述 3 种方法都不能很好地解决复杂网络下 DDoS 欺骗攻击，相应的检测技术已明显滞后于攻击手段的更新。而抵御 DDoS 攻击的核心在于检测，因为只有检测到攻击行为防火墙才能实施包过滤，IDS 才能追踪攻击源，服务器才能拆除虚假连接回收系统资源。如何检测 DDoS 攻击行为，提高算法匹配效率和准确率一直都是研究的难点和热点，也是目前亟待解决的问题。

本文提出一种基于粒子群 BP 神经网络的流量检测模型，结合粒子群算法的全局搜索和遗传算法的快速收敛特性用于检测 DDoS 攻击行为。

2 BP 神经网络自适应学习算法

BP 神经网络的自适应学习性由正向传播和反向传播构成。正向传播时数据从输入层流经各个隐含层处理后通过输出层输出结果。若期望值与输出结果偏差大于预设阈值，采用反向传播梯度法调整，重复两个过程直到偏差小于预设精度为止，从而学习和存储大量的输入输出映射关系，算法如下。

(1)初始化神经网络向量。BP 网络通过反复改变输入权值，使输出结果不断接近最优值。若输入层有 n 个神经元，隐含层有 p 个神经元，输出层有 q 个神经元，变量定义如下：

输入向量：$\boldsymbol{X}=(X_1,X_2,\cdots,X_n)$

隐含层输入向量：$\boldsymbol{h}_i=(h_{i1},h_{i2},\cdots,h_{ip})$

隐含层输出向量：$\boldsymbol{h}_o=(h_{o1},h_{o2},\cdots,h_{op})$

输出层输入向量：$\boldsymbol{y}_i=(y_{i1},y_{i2},\cdots,y_{iq})$

输出层输出向量：$\boldsymbol{y}_o=(y_{o1},y_{o2},\cdots,y_{oq})$

期望输出向量：$\boldsymbol{d}_o=(d_1,d_2,\cdots,d_q)$

样本数据个数：$k=1,2,\cdots,m$

给各连接权值赋予区间$[-1,1]$内随机数，给定计算精度值 ε 和最大学习数 M，计算误差函数 e 为：

$$e=\frac{1}{2}\sum_{o=1}^{q}(d_o(k)-y_o(k))^2 \tag{1}$$

(2)随机选取第 k 个输入样本和期望输出结果：

$$x(k)=\{x_1(k),x_2(k),\cdots,x_n(k)\}$$
$$d_o(k)=\{d_1(k),d_2(k),\cdots,d_q(k)\} \tag{2}$$

(3)计算隐含层各神经元的输入和输出：

$$h_{oh}(k)=f(h_{ih}(k)),h=1,2,\cdots,p$$
$$y_{oo}(k)=f(y_{io}(k)),o=1,2,\cdots,q \tag{3}$$

(4)结合期望结果和实际输出值，计算误差函数对输出层各神经元的偏导数 $\delta_o(k)$：

$$\frac{\partial y_{io}(k)}{\partial w_{ho}}=\frac{\partial(\sum_{h}^{p}w_{ho}h_{oh}(k)-b_o)}{\partial w_{ho}}=h_{oh}(k) \tag{4}$$

(5)利用隐含层到输出层的连接权值、输出层的 $\delta_o(k)$ 输出计算误差函数，修正连接权值：

$$w_{ho}^{N+1}=w_{ho}^{N}+\eta\delta_0(k)h_{oh}(k) \tag{5}$$

(6)利用隐含层各神经元的 $\delta_h(k)$ 和输入参数修正连接权值，计算全局误差：

$$E=\frac{1}{2m}\sum_{k=1}^{m}\sum_{o=1}^{q}(d_o(k)-y_o(k))^2 \tag{6}$$

(7)判断误差是否小于预设精度或最大迭代次数，满足条件则输出计算结果，否则返回到步骤(3)，选取下一个学习样本进入下一轮学习。

通过大量实例样本学习，BP 神经网络的自适应学习特性不仅可以检测出流量中的 DDoS 攻击，还能识别未知攻击行为，从而克服传统依赖特征库匹配才能检测 DDoS 攻击的局限性。对 DARPA 2000 年数据分析表明，BP 神经网络能准确检测间歇式 DDoS 流量攻击。为此，攻击者攻击手段也随之发生变化，从传统的恒速攻击和间歇式攻击转变为流量渐增式攻击和间歇式与速率渐增式组合攻击。此时，该方法需要学习流量中更多样本才能识别攻击行为，收敛速度慢，预设精度容易使算法陷入局部最优现象，影响检测率和误报率。

3 粒子群算法

粒子群算法(PSO)是基于鸟类群体行为研究的模拟算法。鸟群在封闭空间随机搜索食物，并且在这个空间只有一个全局最优值。假如所有鸟都知道当前位置与搜索食物之间距离，那么找到全局最优解的最优方案就是从身边最近的鸟周围区域进行搜寻[2]。在粒子群算法中，寻找最优问题的每个解对应搜索空间的每只鸟，称为粒子。每个粒子的初始化向量代表鸟的飞行位置和速度，每个粒子通过寻找附近粒子迭代搜寻最优解，具体算法如下。

假设在一个 D 维搜索空间中有 N 个粒子组成的粒子群 $\boldsymbol{X}=(X_1,X_2,\cdots,X_n)^{\mathrm{T}}$，其中第 i 个粒子位置为 $\boldsymbol{X}_i=(X_{i1},X_{i2},\cdots,X_{iD})^{\mathrm{T}}$，速度为 $\boldsymbol{V}_i=(V_{i1},V_{i2},\cdots,V_{iD})^{\mathrm{T}}$，第 i 个粒子极值为 $\boldsymbol{P}_i=(P_{i1},P_{i2},\cdots,P_{iD})^{\mathrm{T}}$，种群全局极值为 $P_g=(P_{g1},P_{g2},\cdots,P_{gD})^{\mathrm{T}}$，每个粒子找到下一粒子后按以下公式更新当前位置和速度：

$$v_{id}^{k+1}=wv_{id}^{k}+c_1\mathrm{rand}_1^{k}(p_{id}^{k}-x_{id}^{k})+c_2\mathrm{rand}_2^{k}(p_{gd}^{k}-x_{gd}^{k}) \tag{7}$$

$$x_{id}^{k+1}=x_{id}^{k}=v_{id}^{k+1} \tag{8}$$

$$w(k)=w_{\max}-k\times\frac{(w_{\max}-w_{\min})}{k_{\max}} \tag{9}$$

其中，k 表示迭代次数，c_1 和 c_2 为加速系数，rand 是$[0,1]$区间选取的随机数，p_{id}^{k} 是第 i 个粒子的个体极值在第 d 维的分量，p_{gd}^{k} 是群体全局极值在第 d 维的分量，x_{id}^{k} 和 v_{id}^{k} 分别是第 i 个粒子经 k 次迭代后的第 d 维位置和速度，w 是粒子保持运动惯性权重。粒子通过不断更新当前位置和速率最终找到全局最优解，完成搜索过程。

4 粒子群遗传算法在 BP 神经网络中的应用

BP 网络在检测 DDoS 攻击中需要事先建立网络正常流量参考标准，初始化权值和阈值参数难以确定，设置过小会使算法难以收敛，过大会陷入局部最优。在复

杂网络中 DDoS 攻击具有间歇式和流量渐增式特点，攻击行为和流量特征往往不是简单的一对一等价关系，导致无法检测未知行为攻击。而 PSO 算法全局搜索能力强，但是收敛速度过慢，并且容易陷入局部最优解。因此本文提出基于 BP 网络自适应学习的粒子群遗传算法。

4.1 新算法实现思想

新算法首先通过 PSO 搜索最优位置向量，将网络流量及其参数量化为每个粒子并初始化状态，从而构建神经网络粒子群，找出全局最优极值范围，以此作为 BP 网络的初始阈值，再引入遗传算法和变异算子加速向最优解的收敛速度和避免早熟现象。若得到的结果偏差超出 PSO 提供的预设阈值，再重复搜索过程，直到找出全局最优解。新算法融合 PSO 全局搜索能力、BP 神经网络的学习过程和遗传算法的快速收敛优点，设计步骤如下。

(1)确定 BP 网络隐含层数量，对每一网络流量进行粒子群编码，并进行粒子群初始化。

(2)利用 PSO 算法找出全局最优极值范围，并判断是否满足结束条件(全局极值收敛速度大于偏导数 δ_0 或最大迭代次数)。如果满足结束条件则进入步骤(3)BP 网络学习过程，否则根据式(7)和式(8)更新粒子的速度和位置，并重复本步骤。

(3)将 PSO 找出的全局极值作为 BP 网络的初始阈值并进入学习过程，引入遗传变异算法向最优解加速收敛。

(4)判断结果是否满足条件(群体适应度是否陷入局部最优和结果是否小于极值范围)，如果都满足，则输出最优值；否则返回步骤(2)继续 PSO 算法的全局搜索。新算法流程图 1 所示。

图 1 新算法流程图

4.2 早熟现象判定与处理

PSO 中的粒子当前位置和速度依靠个体极值和全局极值来引导，当粒子发现更优值时，其他粒子受到更优值吸引迅速聚拢，如果集聚点并非全局最优解，表示 PSO 陷入局部最优现象，加上遗传迭代，粒子之间的差异越来越小，导致早熟收敛。由于粒子个体适应度大小是由粒子个体位置和速率决定的，此时可以根据粒子整体适应度状态判断种群是否陷入局部最优。

基于此思想，新算法根据适应度判断是否过早收敛，经过 BP 网络训练后，样本输出的误差总和均值为：

$$\mathrm{fit}(i)=\sum_{s}\sum_{l}(d_l-o_l) \tag{10}$$

其中，s 是输入样本个数，l 是输出层神经元个数。

设粒子群的粒子数目为 N，第 i 个粒子的适应度为当前种群的平均适应度为 f_{il}，当前种群的平均适应度为 f_{avg}，φ^2 为粒子群的群体适应度方差，则 φ^2 可以定义为：

$$\varphi^2=\sum_{i=1}^{N}\left(\frac{f_i-f_{\mathrm{avg}}}{f}\right)^2 \tag{11}$$

其中，f 是归一化定标因子，其作用是限制 φ^2 的大小。在该算法中 f 的取值为：

$$f=\begin{cases}\max|f_i-f_{\mathrm{avg}}|, & \max|f_i-f_{\mathrm{avg}}|>1\\ 1, & 0<\max|f_i-f_{\mathrm{avg}}|<1\end{cases} \tag{12}$$

以上表明，种群适应度方差反映的是种群个体的聚集程度，φ^2 越小，种群个体聚集度越密。随着迭代次数的增加，种群个体适应度差别越小，φ^2 值也随之变小。如果 PSO 算法陷入局部收敛，粒子群粒子就会聚集在空间的一个或几个特定位置，此时，群体适应度方差 φ^2 趋向于零。因此，当 φ^2 大于式(10)给定阈值时即判为早熟收敛现象。为避免这种现象，需要对遗传算子进行变异，变异算子为：

$$p_{gd}^{k}=p_{gd}^{k}+\mathrm{avg}_{d}^{k}\times\mathrm{rand}() \tag{13}$$

其中，avg_{d}^{k} 表示第 k 次迭代变异后粒子在第 d 维位置的平均值：

$$\mathrm{avg}_{d}^{k}=\frac{1}{N}\sum_{i+1}^{\infty}x_{id}^{k} \tag{14}$$

遗传算法的变异算子将群体中优良个体通过交叉和变异操作遗传到下一代，维持种群的多样性，并且可以防止算法过早收敛的现象。

5 实验测试

5.1 流量样本特征采集和建模

本文以 KDD99CUP 作为实验基础数据，通过对样本采集进行训练。本文选取 1 000 个模拟节点，用 Sniffer 抓包采集网络 500 组流量特征样本，其中包含正常的客户机连接请求和间歇式与速率渐增式 DDoS 攻击，典型采样结果如表 1 所示。

从以上 500 组数据量化为 PSO 粒子群并初始化状态参数，选取典型 200 个粒子作为训练数据集，初始化种群微粒个数为 20，测试函数维数分别为 10、20、30，对应的最大迭代次数分别为 500、1 000 和 100，设置初始惯性权重 w=0.9，加速系数 $c1$ 和 $c2$ 为 2.00。网络有 4 个输入节点和 3 个输出节点，确定 BP 网络结构，如图 2 所示。其中 i、j、k 分别代表输入层、隐含层和输出层的

表 1 典型网络流量特征表

服务类型/攻击形式	流量/(bit/ms)	平均方差	周期图	Hurst 参数
Web 服务	3.76 E+04	9.12 E+02	0.764 7	0.221 4
Ftp 服务	6.21 E+05	3.55 E+03	0.352 4	0.127 8
Mail 服务	2.31 E+04	7.92 E+03	0.296 7	0.211 4
SYN flood	2.16 E+04	2.16 E+04	0.854 1	0.652 4
LAND Attack	7.49 E+05	1.62 E+02	0.538 5	0.316 9
TCP 混乱数据包攻击	5.36 E+05	2.33 E+03	0.261 7	0.494 2
EB Server 多连接攻击	4.15 E+04	8.99 E+03	0.154 3	0.562 8
WEB Server 变种攻击	3.22 E+04	6.15 E+04	0.251 9	0.364 8

层数。因此网络中需要寻找 24 个高斯函数中心矢量，6 个基宽向量和 18 个输出层连接权值，共 48 个参数，即算法中的粒子将在 48 维空间搜索满足最小均方误差要求的最优解。

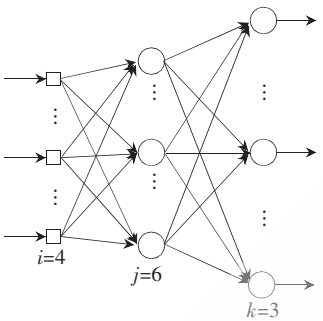

图 2 BP 神经网络结构图

5.2 新算法性能分析

在 MATLAB 2010 的运行环境中，分别采用新算法和 PSO 算法在 10、20、30、40 维的情况下分别运行 200 次，以其平均值作为优化结果。其中最优值用于衡量算法探索能力，均值是在迭代次数内求得最优的平均值，用来衡量算法质量。当平均最优值小于允许误差时即认为搜索成功。实验结果数据如表 2 所示。

表 2 两种算法比较结果

算法	维数	最优值	均值
PSO	10	32.677 5	34.465 2
	20	35.132 6	39.787 9
	30	41.263 1	48.612 4
	40	49.938 2	53.476 3
新算法	10	22.791 2	23.938 5
	20	25.144 9	27.518 6
	30	30.423 2	33.432 4
	40	34.275 2	38.293 8

从表 2 可以看出，在给定迭代次数下，新算法测试结果比 PSO 更接近最优值，计算精度有明显提高，充分体现了新算法的卓越性。

在实验中，PSO 算法参数初始化粒子数为 200，加速因子 $c1=c2=2$，最大迭代次数为 2 000。新算法迭代次数和初始化粒子数等同于 PSO 算法，变异算子中的 rand 取值[0，1]，适应度 P_m 与迭代次数的测试结果如图 3 所示。

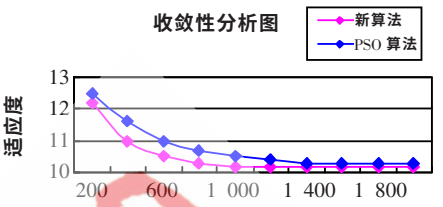

图 3 收敛性分析图

从图 3 可以看出，新算法收敛速度快、误差小，性能明显优于 PSO 算法。当加速因子 $c1=c2=2$ 时，新算法在迭代 1 000 次后无明显变化，找出全局最优解，而 PSO 算法要迭代到 1 450 次左右才趋于稳定，表明新算法通过变异算子向最优解加收敛，搜索的空间复杂度大为减少。

5.3 新算法检测率分析

实验选取 1 000 个模拟节点对服务器发动 SYN flood、LAND attack、TCP 混乱数据包攻击、WEB Server 多连接攻击、Web Server 变种攻击和僵尸网络 DDoS 攻击共 6 种攻击方式，流量上采用渐增式和间歇式组合攻击，测试新算法对攻击行为的检测能力，结果如表 3 所示。

从表 3 数据可以看出，对于带有明显特征的 DDoS 攻击行为（如 SYN Flood 和 LAND Attack），3 种算法检测率和误报率差别不大，新算法略有优势。然而对于未知行为和没有明显特征的 DDoS 攻击行为，如僵尸网络发动的 DDoS 变种攻击，僵尸主机通过伪造虚假 IP 地址发送大量 SYN/ACK 应答，使僵尸网络中攻击端发送的 SYN 请求与 ACK 应答数量达到平衡，攻击特征消失，此时基于特征匹配检测方法几乎失效，PSO 检测率也不高，而新算法优势明显。

新算法结合 PSO 全局搜索、BP 神经网络自适应学习和遗传算法快速收敛的优点，检测 DDoS 攻击行为十分有效，可以检测未知攻击行为，可以将正常行为和攻击行为区别开来，具有较高的检测率和较低的误报率。

参考文献

[1] 李清华，张美凤.基于改进 BP 网络的染色合格率预测[J].微计算机信息，2006(4)：93-95.

[2] 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(3)：38-42.

表 3 渐增式和间歇式组合攻击检测结果

攻击方式	SYN Flood		LAND Attack		TCP 混乱数据包攻击		Web Server 多连接攻击		Web Server 变种攻击		僵尸网络 DDoS 攻击	
检测方率和误报率	检测率/%	误报率/%	检测率/%	误报率/%	检测率/%	误报率/%	检测率/%	检测率/%	检测率/%	误报率/%	检测率/%	误报率/%
特征匹配	84.31	2.25	86.73	2.12	81.49	8.93	72.62	72.62	87.61	2.44	8.36	0.75
PSO 算法	86.27	3.46	85.69	2.62	83.11	6.16	81.72	81.72	86.42	4.84	23.41	1.22
新算法	87.58	2.93	88.32	2.75	96.17	3.93	86.10	86.10	94.26	3.33	78.95	2.13

[3] 危胜军,胡昌振,姜飞.基于BP神经网络改进算法的入侵检测方法[J].计算机工程,2005(13):89-94.

[4] 仲兆满,李存华.基于神经网络的实时入侵检测系统的研究和实现[J].计算机工程与应用,2007(30):126-130.

[5] 易晓梅,陈波,蔡家楣.入侵检测的进化神经网络研究[J].计算机工程,2009(2):103-108.

[6] 潘昊, 侯清兰. 基于粒子群优化算法的BP网络学习研究[J].计算机工程与应用,2006(16):41-43.

[7] 曹承志, 刘洋. 基于改进粒子群算法的BP网络在DTC系统中的转速辨识[J].系统仿真学报,2008(20):77-81.

[8] 宋乃华, 邢清华. 一种新的基于粒群优化的BP网络学习算法[J].计算机工程,2006(14):181-183.

[9] Yu Zhenwe. An automatically tuning intrusion detection system[J]. Systems Man and Cybernetics,2007(2):373-384.

[10] PARIKH D,CHEN T.Data fusion and cost minimization for intrusion detection[J]. Information Forensics and Security, 2008(3):381-389.

[11] BACE M. National institute of standards and technology[J]. NIST Special Publication on Intrusion Detection Systems, 2000(7):76- 79.

[12] LIPPMANN R, CUNNINGHAM R. Improving intrusion detection performance using keyword selection and neural networks[J]. Computer Networks,2000(4):597-603.

[13] RICHARD LIPPMANN, ROBERT K CUNNINGHAM. Improving intrusion detection performance using key word selection and neural networks [J]. Computer Networks, 2000(9):137-144.

[14] LI W, CANINI M, MOORE A. Efficient application identification and the temporal and spatial stability of classification schema[J]. Computer Networks, 2009(7): 252-261.

[15] LI W, CANINI M, MOORE A W. Efficient application identification and the temporal and spatial stability of classification schema [J]. Computer Networks, 2009(6): 790-809.

[16] CHE Z H. PSO-based back-propagation artificial neural network for product and mold cost estimation of plastic injection molding[J]. Computers and Industrial Engineering, 2010(10):236-242.

[17] KENNEDY J. Particle swarm optimization [J]. Neural Networks, 1995(10):236-242.

[18] BAHEER A, HAJMEER M. Artificial neural networks fundamentals [J]. Computing Design and Application, 2000(10):168-175.

[19] SUN J, FENG B. Particle swarm optimization with particleshaving quantum behavior [J]. Evolutionary Computation, 2004(5):232-230.

[20] DORIGO M, BONABEAU E. Ant algorithms and stigmergy[J]. Future Generation Computer Systems, 2000 (11):269-275.

(收稿日期:2013-10-10)

作者简介:

李锋,男,1981年生,硕士,讲师,主要研究方向:网络安全和图像处理。