doi: 103969/j. issn. 0490-6756. 2017. 01. 012

基于 BP 神经网络的 DDoS 攻击检测研究

杨可心[1], 桑永胜[2]
(1. 河海大学企业管理学院, 常州 213022; 2. 四川大学计算机学院, 成都 610065)

摘 要: 分布式拒绝服务攻击(DDoS)是如今常见的网络威胁之一,DDoS 攻击易被发动却很难追踪与防范. 在神经网络快速算法基础上,首先系统分析国内外 DDoS 攻击检测理论、方法与大量数据集,构建了基于数据包长度,数据包发送时间间隔以及数据包长度变化率等六项特征的攻击流量特征模型;其次通过大量尝试提出对神经网络误差调整参数进行优化的方法;最后基于加州大学洛杉矶分校数据集(UCLA CSD Packet Traces)进行了参数改进前后的攻击检测对比实验. 实验表明,本文提出的方法能有效提高 DDoS 攻击检测率,且具有较好的泛化能力.

关键词: BP 神经网络; DDoS 攻击; 入侵检测
中图分类号: TP393. 08 **文献标识码**: A **文章编号**: 0490-6756(2017)01-0071-05

Research on DDoS detection based on BP neural network

YANG Ke-Xin[1], *SANG Yong-Sheng*[2]
(1. School of Business Administration, Hohai University, Changzhou 213022, China;
2. College of Computer Science, Sichuan University, Chengdu 610065, China)

Abstract: Distributed denial of service attack (DDoS) is a common threat in today's networks. While such an attack is not difficult to launch, defending a network resource against it is disproportionately difficult. This paper analysis some famous theories and methods on detection of DDoS network attacks systematically based on the fast neural network algorithm. Meanwhile, the attack traffic feature model which is constructed based on the packet length, packet transmission time interval and packet length change rate etc is proposed. Second, a method to optimize the parameters of the neural network error is also proposed by a large number of attempts. Finally, the UCLA dataset is used to carry out the contrast experiment of the parameters before and after the improvement. Experiments show that the proposed method can effectively detect DDoS attacks and has a better generalization ability.

Keywords: BP neural network; DDoS attack; Intrusion detection

1 引 言

分布式拒绝服务(Distributed Denial of Service attack,DDoS)攻击对网络上的主机,服务器乃至网络基础设施均会造成严重危害[1-3],如 2009 年暴风门事件造成全国大范围断网,2015 年 3 月全球知名软件代码托管网站 GitHub 遭遇持续 80 多小时的大规模 DDoS 攻击以及同年 8 月五家俄罗斯银行遭 DDoS 攻击并被勒索 50 比特币. 攻击者基于敲诈勒索,实施报复,赢得竞争等目的采取这

收稿日期: 2016-04-12
基金项目: 四川省应用基础研究计划项目(2013JY0018)
作者简介: 杨可心(1995-), 女, 四川绵阳人, 研究方向为网络安全. E-mail: yangkexin0528@163. com
通讯作者: 桑永胜. E-mail: sangysh@126. com

种成本低廉的攻击实现长期打击.大多数情况下,攻击者利用 TCP,UDP 和 ICMP 协议发动 DDoS 攻击,致使被攻击公司的业务瘫痪并造成巨大的经济损失.因此,如何实时检测和有效减轻 DDoS 攻击成为近年来重要的研究领域之一.

人工神经网络(artificial neural network,ANN)具有的适应性,自学习以及非线性逼近能力已被广泛应用于预测,建模,分类和自适应控制,且在 DDoS 攻击的检测方面取得了较好的成果.国外研究中,Gupta 等[1]提出一种神经网络检测模型来解决识别低速率攻击时稳定性差的问题.Saied 等[2]用不断更新学习样本方式提高对未知类型的 DDoS 攻击检测率.Kale 等[4]提出结合分类器输出与 Neyman Pearson 成本最小化战略的分类检测算法.Karimazad 等[5]提出 RBP 分类算法提高了攻击检测精度并降低误报率.国内研究中,孙知信等[6]提出了基于聚类和协议分析防御和检测 DDoS 攻击的模型.张永铮等[7]介绍了基于不同网络层次的各种控制与检测方法,并提出 DDoS 攻击过滤系统的未来发展趋势和相关技术难点.杨新宇等[8]提出了一种基于非线性预处理网络流量预测方法 NLPP 的分布式拒绝服务 DDoS 攻击检测算法.牟超等[9]提出了一种基于进化神经网络预测 RNA 二级结构的方法,改善了 BP 神经网络易陷入局部误差等缺陷.吕涛等[10]提出基于 SNMP 与神经网络的检测特征模型进行 DDoS 攻击检测.胡鸿等[11]提出通过 BP 神经网络检测 TCP 缓存异常程度来判断是否发生攻击.董超等[12]基于网络特征行为提出免疫算法提高特征提取速度.任勋益等[13]利用 GA 的全局搜索能力优化 BP 神经网络权值并将其用于异常检测之中.汪洁[14]设计和实现了一个基于蜜罐和 BP 神经网络的入侵检测系统并建立检测模型.

然而由于高速数据速率的限制以及神经网络算法的复杂性等原因,上述文献尽管注意到利用算法改进来提高攻击检测效率问题,但在通过选择算法误差调整参数及分析攻击流量行为模式来优化检测的方面考虑不足.从提高检测的精度及效率,降低误报率等方面考虑时,选择正确的误差调整参数可以在神经网络学习过程减小振荡,加快收敛以及避免陷入局部陷阱,而选择显著的攻击流量特征可以提高神经网络识别率.本文在前人研究的神经网络快速算法[15]的基础上,首先系统分析国内外 DDoS 攻击检测理论、方法与大量数据集,构建了基于数据包长度,数据包发送时间间隔以及数据包长度变化率等六项特征的攻击流量特征模型,其次通过大量尝试提出对神经网络误差调整参数进行优化的方法,实验表明,本文提出的方法能加速神经网络的学习过程并有效提高 DDoS 攻击检测准确率.因此,能将其有效地应用到网络安全领域.

2 多层神经网络快速算法

在使用最速下降法来训练一个运用 sigmoid 函数的多层神经网络时,可能因为梯度的幅度过小导致权重和偏差变化较小,甚至远离它们的最优值.而快速算法能较好解决这种局部误差陷阱问题.三层神经网络的网络结构如图 1 所示.

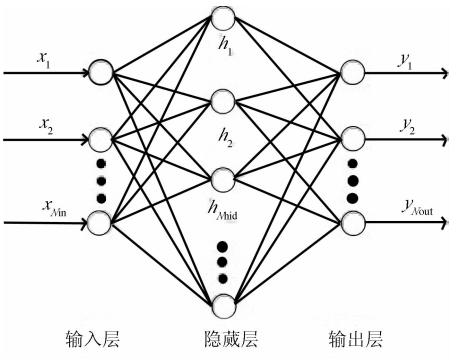

图 1 三层神经网络结构图

Fig. 1 The structure of the three layer neural network

其中,我们作如下定义,N_{in},N_{hid} 和 N_{out} 分别为输入层,隐藏层和输出层的神经元数;Wih_{ij} 为输入层第 i 个神经元到隐藏层第 j 个神经元的连接权;Who_{jk} 为隐藏层第 j 个神经元到输出层第 k 个神经元的连接权.

由此,设输入模式数为 L,输入项量为 $x_L=[x_{L1},x_{L2},\cdots,x_{LN_{\text{in}}}]$,隐藏向量为 $h=[h_1,h_2,\cdots,h_{N_{\text{hid}}}]$,实际输出向量为 $y_L=[y_{L1},y_{L2},\cdots,y_{LN_{\text{out}}}]$,期望输出向量为 $t_L=[t_{L1},t_{L2},\cdots,t_{LN_{\text{out}}}]$,且 $f(x)=\text{sigmoid}(x)$,则快速算法的详细描述如算法 1 所示.

算法 1 神经网络快速算法

Begin

Initializing: $Wih,Who,\mu,g,\lambda,\eta,E_0$

Foreach sample Do (1.0)

forward: (1.1)

Hidden layer: $h_j=f(\sum_{i=1}^{N_{in}}Wih_{ji}x_i)$

Output layer: $y_k=f(\sum_{j=1}^{N_{hid}}Who_{kj}h_j)$

backward：　　(1.2)

Output layer error：

$\delta_k^{\text{out}}(\lambda)=t_k-\lambda y_k$

Hidden layer error：

$$\delta_j^{\text{hid}}(\lambda)=(1-h_j^2)\sum_{k=1}^{N_{\text{out}}}\delta_k^{\text{out}}(\lambda)Who_{kj}$$

Edge weight：

$Who_k=Who_k+\eta\delta_k^{\text{out}}(\lambda)h_k$

$Wih_j=Wih_j+\eta\delta_j^{\text{hid}}(\lambda)x_i$

Hidden layer：$h_j=f(\sum_{i=1}Wih_{ji}x_i)$

Output layer：$y_k=f(\sum_{k=1}Who_{kj}h_j)$

Then $E=E+\frac{1}{2}\sum_k(t_k-y_k)^2$　　(2.0)

If $E>E_0$；$\lambda=\exp(-\mu/E^g)$；back to(1.0)；else end；

End.

3　流量分类规则及标准化特征提取

选择有效的输入特征能够提高 DDoS 攻击检测的准确率. 由于攻击者的目的是最大化破坏目标网络或系统的处理能力，那么所采用的检测方法不能消耗过多资源而加重网络或系统的负担. 因此在特征提取时，应选择具有代表性且易于测量的统计功能.

通过对大量数据集的观察，并且进一步分析数据集中协议标识、源 IP 地址、目的 IP 地址、序列号等可描述数据包特征的信息，找到了能证明 DDoS 攻击流量存在的一些显著特征. 考虑到统计的方便，最终选择了以下特征.

(1) 数据包总数. 输入数据包总数的异常高值是 DDoS 攻击最明显的特征. 由于其简单性，通常用于检测机制.

(2) 数据包总长度. 本文观察到在 DDoS 攻击时数据包总长度大幅上升明显高于正常值，由此该特征可用于判断攻击. 在统计时采用下式对数据进行处理，从而提高准确性.

$$y=\frac{x-\text{Min}Value}{\text{Max}Value-\text{Min}Value}\qquad(1)$$

其中，x、y 分别为某一样本转换前、后的值，Max*Value*、Min*Value* 分别为样本中数据包总长度的最大值和最小值.

(3) 发送数据包时间间隔. DDoS 攻击通常表现为突发性短时间内传入数据包数量的急速上增，因此时间间隔对于判断攻击具有重要意义. 统计时采用计算相邻数据包发送的平均时间间隔的方式进行量化.

(4) 数据包长度变化率. 研究发现，攻击数据包的长度几乎一致，而正常的数据包即使属于同一文件也不相同. 由此规定样本中数据包长度几乎一致的变化率为 0.01 而几乎不同为 1.00，并采用公式 $y=x/\text{SUM}$ 进行处理，其中 y 为转换后的值，x、SUM 分别为某一样本中相同数据包个数和数据包总数.

(5) 数据包传送速率. 这个特性显示了在一个特定的时间跨度内从一个源地址到目的地址传送的数据包个数. 在攻击的时间里可以观察到传送速率大幅增加. 在统计时设定时间窗口为 0.5 s 并统计样本中相同时间间隔中传送数据包的平均个数.

(6) 数据包协议标识. TCP 包均带有 flag 标记. 通过实验观察到正常数据包带有标记种类高于异常数据包，统计时通过公式来量化这一特征：$y=$样本中协议标志种类数/TCP 协议中协议标志种类总数，其中，y 为转换后的值.

4　DDoS 攻击流量检测实验

在实验时，本文选取了加州大学洛杉矶分校数据集(UCLA CSD Packet Traces)，并使用其中一段 TCP 数据包的网络流量记录来进行样本提取与特征分析. 包含正常流量与攻击流量的数据集是由该校分布网络研究实验室于 2008 年在实验中运行 TFN 攻击工具时跟踪采集得到，利用这种混合流量进行研究确保了本文研究的真实性与准确性.

4.1　实验样本采集

在样本采集时，捕获了数据集中 14.02 s 内的 11243 个 TCP 数据包，抽取十组样本进行统计并分类. 结果表明，在第 3 节中提出的特征包含了有关 DDoS 攻击存在的大量信息. 例如攻击流量的数据包长度变化率几乎都为 0.01，这是为了达到短时间内产生大量无效数据包的目的而设置的. 表 1 对样本提取的结果进行了总结. 在运用神经网络进行实验之前，对以上输入值进行了归一化处理从而提高检测的准确性. 如果对输入值不处理就直接应用，那么大的值可能会抑制较小的值的影响. 在第 3 节提出的处理方法的基础上，对样本进行了归一化处理以方便在实验中的使用.

4.2　参数设置

针对第 2 节提出的算法以及第 3 节特征提取结果，选择了 6 个输入节点，15 个隐藏节点，10 个

表 1 样本提取结果

Tab. 1 The results of sample extraction

编号	源 IP	目的 IP	总数	总长度(比特)	时间间隔(s)	变化率	包率(0.5s)	标志	分类
1	11.1.8.15	15.11.94.12	51	3009	0.3	0.9	3	0.22	正常
2	17.1.50.100	1.1.4.4	32	1600	0.5	0.4	3	0.22	正常
3	49.243.102.52	1.1.4.4	28	1232	0.6	0.7	3	0.22	正常
4	24.43.192.185	1.1.4.4	30	1110	0.55	0.8	2	0.22	正常
5	8.8.11.11	1.1.4.4	29	1363	0.5	0.8	2	0.22	正常
6	44.177.143.20	1.1.17.60	668	92528	0.001	0.01	35	0.15	攻击
7	24.176.9.212	1.1.54.134	470	9400	0.01	0.01	20	0.11	攻击
8	9.3.22.181	1.1.39.36	500	22000	0.001	0.01	25	0.11	攻击
9	22.17.21.217	1.1.35.39	122	178120	0.11	0.01	40	0.11	攻击
10	38.182.100.129	1.1.17.219	366	534360	0.004	0.01	55	0.22	攻击

输出节点的 BP 神经网络. 实验将 50%的数据用于训练神经网络以及 50%用于攻击检测,并对比了算法改进前后的结果. 在进行大量尝试之后,当参数设置为表 2 时可得到两种算法的最高效率.

表 2 实验参数设置

Tab. 2 The experimental parameter settings

算法种类	学习率	g	μ	隐层误差校正系数
传统的三层 BP 神经网络	0.7	无	无	$(1-h_j)h_j$
改进后的三层 BP 神经网络	0.7	0.2	0.1	$(1-h_j^2)$

4.3 结果对比

本小结通过实验对本文算法的效率和精度进行了测试,实验结果在表 3 与图 2 中给出。

表 3 识别结果对比

Tab. 3 The comparison of recognition results

算法种类	平均耗时(ms)	平均学习次数	准确率
传统的三层 BP 神经网络	3027	2269	97%
改进后的三层 BP 神经网络	1497	919	98.1%

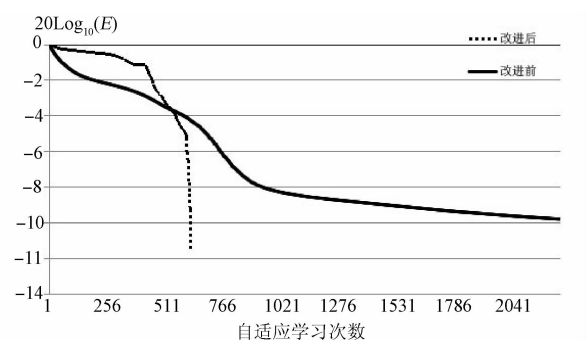

图 2 收敛性对比

Fig. 2 The comparison of convergence

表 3 的实验结果显示,本文所提出的改进算法在平均迭代次数上减少幅度达到了 50%以上. 因此改进后的算法可以显著地缩短 CPU 计算时间,提高 DDoS 攻击检测的效率. 同时,改进后的算法在平均入侵检测精度上也有明显改善,提高了约 1.1%. 我们在图 2 中给出了算法的收敛性对比实验结果. 图 2 中,采用自适应学习次数为自变量,$20\log_{10}(E)$ 为因变量(E 为总误差),观察方法改进前后的收敛性变化. 从图 2 中,我们可以清楚地看出,改进后的算法其误差在约 490 次学习后快速下降,收敛速度明显优于改进前. 对比实验表明,改进的神经网络算法是收敛的,并且提升了算法的收敛速度,可以改善实际工程应用中 DDoS 攻击检测的实时性.

5 结 论

在神经网络快速算法基础上,本文设置了特定的神经网络误差参数并提取攻击流量的特征运用于基于 TCP 的 DDoS 攻击检测,取得了较好的效果. 对于数据集,采用了加州大学洛杉矶分校分步网络研究实验室采集的 TCP 攻击流量数据集以确保计算结果的真实性与准确性. 在实验时对提取样本进行归一化处理,并用 c++对神经网络快速算法进行了实现. 通过对改进前后算法结果的对比研究,证明了本文提出的方法能有效提高检测效率以及准确率. 然而考虑到提取用于检测的数据的有限性,将在今后的工作中将使用大量的 TCP 数据进行实验,进一步完善现有的研究.

参考文献:

[1] Gupta B B, Joshi R C, Misra M. ANN based scheme to predict number of zombies in a DDoS at-

tack[J]. Int J NS, 2012, 14(2): 61.

[2] Saied A, Overill R E, Radizk T. Artificial neural networks in the detection of known and unknown DDoS attacks: proof-of-concept[C]//Proceedings of PAAMS 2014 International Workshops. Salamanca, Spain: PAAMS, 2014.

[3] Oke G, Loukas G, Gelenbe E. Detecting denial of service attacks with bayesian classifiers and the random neural network [C]//Proceedings of the IEEE International Conference on Fuzzy Systems. London, Britain: IEEE, 2007.

[4] Kale M, Choudhari D M. DDoS attack detection based on an ensemble of neural classifier[J]. IJCSNS, 2014, 14(7): 122.

[5] Karimazad R, Faraahi A. An anomaly-Based method for DDoS attacks detection using RBF neural networks[C]//Proceedings of 2011 1st International Conference on Network and Electronics Engineering. Singapore: IACSIT, 2011.

[6] 孙知信，姜举良，焦琳. DDOS 攻击检测和防御模型[J]. 软件学报，2007，18(9)：2245.

[7] 张永铮，肖军，云晓春，等. DDoS 攻击检测和控制方法[J]. 软件学报，2012，23(8)：2058.

[8] 杨新宇，杨树森，李娟. 基于非线性预处理网络流量预测方法的泛洪型 DDoS 攻击检测算法[J]. 计算机学报，2011，34(2)：395.

[9] 牟超，何静媛，石杨. 基于进化神经网络的 RNA 二级结构预测方法[J]. 四川大学学报：自然科学版，2014，51(1)：64.

[10] 吕涛，禄乐滨. 基于 SNMP 和神经网络的 DDoS 攻击检测[J]. 通信技术，2009，42(3)：189.

[11] 胡鸿，袁津生，郭敏哲. 基于 TCP 缓存的 DDoS 攻击检测算法[J]. 计算机工程，2009，35(16)：112.

[12] 董超，周刚，刘玉娇，等. 基于改进的 Adaboost 算法在网络入侵检测中的应用[J]. 四川大学学报：自然科学版，2015，52(6)：1225.

[13] 任勋益，王汝传，周何骏. 遗传 BP 神经网络及其在异常检测中的应用[J]. 计算机工程与科学，2008，30(11)：19.

[14] 汪洁. 基于神经网络的入侵检测系统的设计与实现[J]. 计算机应用与软件，2013，30(5)：320.

[15] 冯昭志，黄载禄，杨叔子. 单层神经网络的快速学习算法研究[J]. 自动化学报，1997(1)：68.