一种基于神经网络的入侵检测技术

薛 俊[1,2], 陈 行[1,2], 陶 军[1,2]
(1.东南大学 计算机科学与工程学院,江苏 南京 210096;
2.东南大学 计算机网络与信息集成教育部重点实验室,江苏 南京 210096)

摘 要:应用神经网络技术不仅能识别已知的网络入侵行为,而且也能识别许多未知的网络入侵的变种。BP神经网络是一种成功的神经网络技术,然而,标准BP算法学习速率固定,不能根据实际情况动态改变学习速率。为了自适应当前网络学习的状况,提高网络的收敛速度,提出了一种基于综合增加动量项与自适应调节学习速率相结合的改进BP算法,可以满足入侵检测分类识别的需求。选用Kddcup 1999 Data网络连接数据集进行特征提取和预处理之后,送入神经网络进行训练和测试,得到较高的检测率和较低的误报率。实验表明,基于改进的BP神经网络的入侵检测方法是有效的。

关键词:入侵检测;BP算法;检测率;误报率
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)08-0148-03

Technology of Intrusion Detection Based on Neural Network

XUE Jun[1,2], CHEN Hang[1,2], TAO Jun[1,2]
(1. School of Computer Science & Engineering, Southeast University, Nanjing 210096, China;
2. Ministry of Education Key Lab. of Computer Network & Information Integration, Southeast University, Nanjing 210096, China)

Abstract: Neural network can recognize the known action of network attacks as well as the unknown variation of the known network intrusion. Neural network based on BP algorithm is a kind of successful technology. However, the learning rate of the standard BP algorithm is static, and cannot be adjusted dynamically according to current real situation. In order to self-adjust the current studying status of neural network and enhance the speed of convergence of network, here present and apply the improved BP algorithm combined a method of adding momentum item(s) with the self-adjusting learning rate in the paper. The improved BPNN can meet the needs of classified recognition of IDS. Experiments with KDD CUP 1999 network traffic connections which have been preprocessed after feature abstraction have shown that the improved BPNN is effective for intrusion detection owing to good performance of the higher attack detection rate and the lower false positive rate.

Key words: intrusion detection; BP algorithm; ADR; FPR

0 引 言

入侵检测是信息安全技术的重要组成部分,是一种事后处理方案,具有智能监控、实时检测、动态响应、相对易于配置的特点。根据被检测数据来源分类,入侵检测技术分为基于主机(host-based)的入侵检测和基于网络(network-based)的入侵检测[1]。基于主机的入侵检测系统的检测对象通常是操作系统下的安全记录及系统记录;基于网络的入侵检测系统使用原始网络数据包作为检测对象。根据检测方法分类,入侵检测技术可分为滥用检测(Misuse Detection)与异常检测(Anomaly Detection)[1]。滥用检测根据已知的入侵攻击信息匹配被检测数据,它只能确定已知攻击;异常检测建立系统正常行为的轨迹,把所有偏离正常轨迹的系统状态视为可疑企图,但并非所有的入侵都表现为异常,系统的轨迹难于计算和更新。

一些研究人员利用数据挖掘方法[2,3]、数据融合技术[4~6]等来进行入侵检测和网络流量预测的研究。从实际应用看,大多数入侵检测系统都是基于滥用的,但它不能检测出已知攻击的变种。由于神经网络具有的概括和抽象能力,通过对样本的不断学习,其应用在入侵检测方面能得到较好的效果[7~9]。因此,笔者提出一种基于改进的BP神经网络的入侵检测方法,能一定程度克服滥用入侵检测系统的缺点。实验表明,

收稿日期:2008-12-26;**修回日期**:2009-03-23
基金项目:国家自然科学基金重大研究计划项目(90604003)
作者简介:薛 俊(1979-),男,江苏南京人,硕士研究生,研究方向为网络安全、网络入侵检测、神经网络;导师:吴国新,教授,博士生导师,从事计算机网络及其应用方面的研究和教学工作。

改进的 BP 神经网络用于入侵检测,效果良好,为实现入侵检测系统提供了一条良好的途径。

1　改进的 BP 学习算法

BP 学习算法的核心任务就是要使目标函数以尽可能快的速度达到所要求的一个小的正数值,实现多层前向神经网络的实际输出和期望输出的数值拟合。通常将目标函数定义为 $E=\frac{1}{2}(D-O)^2=\frac{1}{2}\sum_{k=1}^{l}(d_k-o_k)^2$,其中 $D=(d_1,\cdots,d_l)^{\mathrm{T}}$ 为期望输出,$O=(o_1,\cdots,o_l)^{\mathrm{T}}$ 为实际输出。然而,传统 BP 算法是标准的梯度法,算法学习速率固定,不能根据实际情况动态改变学习速率。为了自适应当前网络学习的状况,提高网络的收敛速度,文中提出了综合增加动量项与自适应调节学习速率相结合的改进算法,能自适应调整网络学习速率,从而有效提高算法的效率。概括起来,改进的算法可描述如下:

(1) 初始化:定义目标函数输出为 E,上一次目标函数输出 preE ← 较大的正数;权值矩阵各元素 $w_{kj}(t)$、$v_{ji}(t)$ ← random(−1, +1),$(k=1,\cdots,l;\ j=0,\cdots,m;\ i=0,\cdots,n)$;$\Delta w_{kj}(t)$、$\Delta v_{ji}(t)$ ← 0 为算法迭代相邻两次同一权值的调整量;当前学习样本号 p ← 1,P ← 总的学习样本数,学习轮次数 q ← 1;误差和 E_T ← 0;迭代步 t ← 0,学习率 $\eta(t)$ ← (0,1) 间的一个常数,动量因子 α ← 小的正常数 (< 1)。

(2) 输入第 p 个样本:输入向量 $(x_1,x_2,\cdots,x_n)$,期望输出 $(d_1,d_2,\cdots,d_l)$。记 x_i,y_j,o_k 分别表示输入向量第 i 个分量,隐层第 j 个神经元输出分量,输出信号第 k 个分量。对于输出层,$o_k=f(\mathrm{net}_k)$,$\mathrm{net}_k=\sum_{j=0}^{m}w_{kj}(t)y_j$ $(k=1,\cdots,l)$;对于隐层,$y_j=f(\mathrm{net}_j)$,$\mathrm{net}_j=\sum_{i=0}^{n}v_{ji}(t)x_i$ $(j=1,\cdots,m)$,其中 $f(x)=\frac{1}{1+e^{-x}}$ 为单极性 sigmoid 函数。

(3) 按目标函数的定义计算 E,并加到误差和 E_T;迭代步 t 自加 1。当 $E\geqslant$ preE 时,$\eta(t)=\theta\eta(t-1)$,$(\theta<1)$;当 $E<$ preE 时,$\eta(t)=\beta\eta(t-1)$,$(\beta>1)$;preE ← E。

(4) 计算各输出层神经元误差信号:$\delta_k^o=o_k(1-o_k)(d_k-o_k)$,各隐层神经元误差信号:$\delta_j^y=y_j(1-y_j)\sum_{m=1}^{l}\delta_m^o w_{mj}(t-1)$,$(k=1,\cdots,l;j=1,\cdots,m)$。

(5) 调整权值矩阵:

$\Delta w_{kj}(t)=\eta(t)\delta_k^o y_j+\alpha\Delta w_{kj}(t-1)$,$w_{kj}(t)=w_{kj}(t-1)+\Delta w_{kj}(t)$;

$\Delta v_{ji}(t)=\eta(t)\delta_j^y x_i+\alpha\Delta v_{ji}(t-1)$,$v_{ji}(t)=v_{ji}(t-1)+\Delta v_{ji}(t)$;

$(k=1,\cdots,l;j=0,\cdots,m;i=0,\cdots,n)$。

(6) 当不是所有 P 个训练样本都训练完毕,$p\leftarrow p+1$,返回(2);否则,到(7)。

(7) $E_{\mathrm{avg}}=E_T/P$,若 $E_{\mathrm{avg}}<=$ 规定的要求,算法结束;否则 $E_T\leftarrow 0$,$q\leftarrow q+1$,$p\leftarrow 1$,返回(2)。

2　入侵检测原型设计

基于网络的入侵检测系统(NIDS),通过对来自网络的数据流量来检测入侵的行为。它提取网络连接的相关信息,对每一连接进行预先处理后送入已被训练过的神经网络模块,判断其是正常数据还是非正常数据。原型抽象图如图 1 所示。

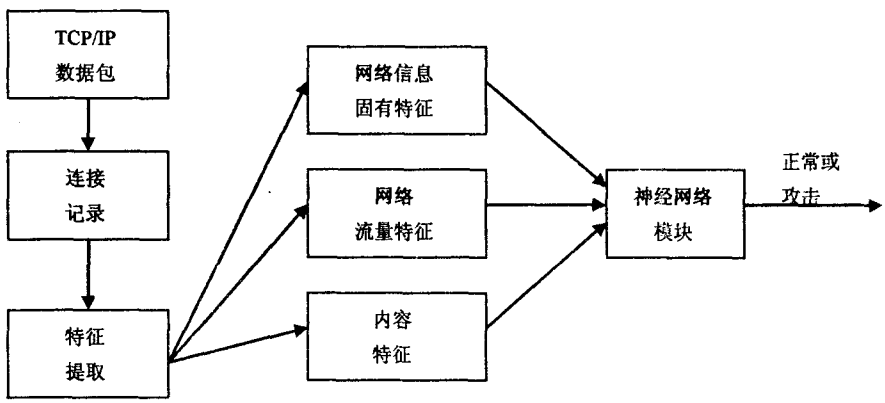

图 1　原型抽象图

图 1 可分为三个模块组成,分别是数据采集模块、数据预处理模块、神经网络模块。

2.1　数据采集模块

包括图 1 中“TCP/IP 数据包”、“连接记录”框。它收集被检测网络中的数据流,还原成一个个连接记录,供特征提取模块利用。连接记录是通信双方一次会话之间的一系列的单向数据包。

2.2　数据预处理与特征提取模块

包括图 1 的“特征提取”、“网络信息固有特征”、“网络流量特征”、“内容特征”框,通过这些特征,能区分正常的网络行为和异常行为。将这些特征信息预处理后转化成神经网络可识别的形式送入神经网络模块学习或识别。

* 固有特征:连接的通用信息。

* 流量特性:与当前连接有相关性的过去的连接的统计信息。

* 内容特征:关于数据包数据负载的信息特征。

2.3 神经网络模块

它在学习阶段接受由预处理模块输入的学习样本,用改进 BP 学习算法调整网络神经元之间的权值;在检测阶段,训练好的神经网络计算输入的数据记录,判断是否是正常网络行为或某类型的攻击并输出判断结果。

3 入侵检测实验测试

3.1 实验数据源简介

实验数据采用 DARPA 1999[10]入侵检测评估数据集作为训练数据和测试数据,每条记录包含 41 个特征。从数据集中随机抽取了 2402 条包含 4 类攻击(smurf、ipsweep、buffer_overflow、guess_passwd)和正常的连接记录,前一半作为训练,整个 2402 条作为测试。其中正常连接 598 条,攻击连接 1804 条。基于网络和主机的攻击与以下十五项数据集的特征字段联系紧密:Duration, Protocol type, Service, num_failed_logins, logged_in, hot, Count, Serror_rate, Rerror_rate, Same_srv_rate, Diff_srv_rate, Srv_count, Srv_serror_rate, Srv_rerror_rate, Srv_diff_host_rate。将以上十五项预处理后输入神经网络学习或测试。

3.2 改进的 BP 算法与传统 BP 算法的性能比较和实验结果

神经网络采用输入层节点数 15 个,第一隐层 25 个节点,第二隐层 15 个节点,输出层 5 个节点。改进的 BP 算法的初始学习速率 $\eta(0)=0.25$,动量因子 $\alpha=0.075$,初始权值为(-1.0,1.0)之间的随机数。为了与改进 BP 算法比较,除了不存在动量因子外,标准 BP 算法的其余初始条件同改进算法。实验环境采用 Intel CPU,主频 2.13GHz,512MB 主存,Windows XP 操作系统。图 2 给出了同样经过 1000 次的训练过程,改进算法与传统算法的学习次数—输出误差曲线图。由图可推知,当设置同一训练结束条件时,改进算法比传统算法收敛的快。

表 1 为改进算法、传统算法在同样训练迭代次数的条件下输出误差的比较和在相同的训练结束条件下收敛花费的时间比较。

表 2 是应用改进 BP 算法对测试数据进行测试的结果,显示对于检测率 ADR(Attack Detection Rate)[1]、误报率(False Positive Rate)[1]得到了较理想的结果。

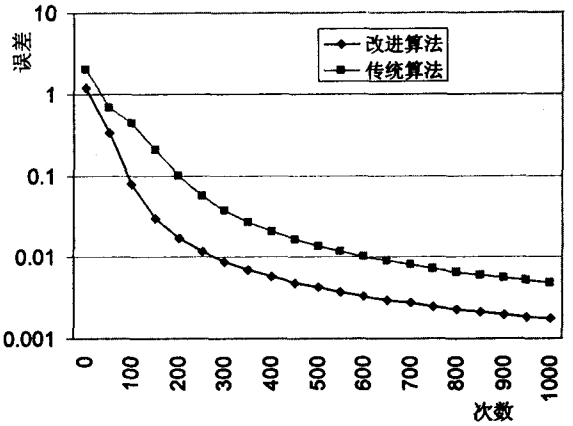

图 2 改进算法、传统算法的学习次数——输出误差曲线图

表 1 改进算法、传统算法误差、训练时间的比较

输出平均误差(迭代 5000 次后)		训练时间(误差小于 0.001 时结束,1200 条训练记录)	
改进算法	传统算法	改进算法	传统算法
0.000098	0.000244	43.63 秒	84.71 秒

表 2 改进 BP 算法测试结果的交叉矩阵

实际 \ 预测	normal	smurf	ipsweep	buffer_overflow	guess_passwd	未知
normal	542	0	13	16	9	18
smurf	0	907	29	0	0	38
ipsweep	28	0	589	0	1	42
buffer_overflow	2	0	1	69	0	9
guess_passwd	2	1	8	1	72	5

由上表可得检测率 ADR 为 90.7%,误报率 FPR 为 9.36%。也就是说,大部分的入侵攻击可以被系统检测到,大部分的正常行为也可被系统识别,证明基于改进的 BP 神经网络的入侵检测的性能是优良的。

4 结束语

阐述了改进 BP 算法应用于入侵检测。实验表明改进 BP 算法缩短了训练时间,在测试时具有较高的检测率和较低的误报率,得到了较为理想的结果,是用于入侵检测引擎的可行方案。在下一步,将把神经网络模型与模式匹配技术相融合应用于检测引擎并对实际的网络流量进行检测。

参考文献:

[1] 曹元大.入侵检测技术[M].北京:人民邮电出版社,2007.

[2] 顾健辉,孙力娟.数据挖掘技术在入侵检测中的应用研究[J].计算机技术与发展,2006,16(9):243-245.

[3] Lee Wenke, Stolfo S, Mok K. A Data Mining Framework for Building Intrusion Detection Models[C]//IEEE Symposium

(下转第 154 页)

3 实验分析

对实验中应用逻辑做如下安排：task0 每隔 5s 向消息队列申请一个消息，而 task1 每隔 3s 向消息队列发送一个消息。首先采用 μC/OS－II 原有消息队列的处理方式以验证 1.2 中提出的 μC/OS－II 中存在的数据安全性问题，其运行结果如图 3 所示。

```
task1 has send message:message0
task0 has received message:message0
task1 has send message:message1
task1 has send message:message2
task0 has received message:message2
task1 has send message:message3
task0 has received message:message3
task1 has send message:message4
task1 has send message:message5
task0 has received message:message5
```

图 3 使用 μC/OS－II 原消息队列机制的运行结果

从图 3 可见由于 task0 没能在 task1 发送下一个消息之前从消息队列中取走 task1 前一次发送的消息，message2 和 message5 分别覆盖了 message1 和 message4。接下来采用改进后的消息队列处理方式来验证所做改进的正确性和有效性，其运行结果如图 4 所示。

```
task1 has send message:message0
task0 has received message:message0
task1 has send message:message1
it's not safe now,I have to wait
task0 has received message:message1
task1 has send message:message2
task0 has received message:message2
task1 has send message:message3
it's not safe now,I have to wait
task0 has received message:message3
task1 has send message:message4
it's not safe now,I have to wait
task0 has received message:message4
task1 has send message:message5
task0 has received message:message5
```

图 4 使用改进后的消息队列机制的运行结果

从图 4 可见改进后的消息队列机制确实能保证数据的安全性，这一安全性的保证需要应用函数在不确定修改消息是否安全时通过调用 OSQTest 函数进行查询，当然查询会额外消耗一定的时间，但是从第 2 节中 OSQTest 的源代码可以看出这一查询时间是相当短的，因此在安全性要求较高的环境中使用这一查询是值得的。

4 结束语

文中分析了 μC/OS－II 中消息队列通信机制的实现原理以及其中存在的数据安全性问题，通过改进消息队列通信涉及的数据结构，增加相应的系统函数，从而增强了 μC/OS－II 中消息队列通信的数据安全性。最后通过实验证明以上改进在实际应用中的有效性。

参考文献：

[1] 胡修林，杨 刚，张蕴玉，嵌入式多任务操作系统中的任务间通信策略[J]. 自动化技术与应用，2004(7)：39－42.

[2] 员 青，钱 锋，田蔚凤. 占先式实时内核 μC/OS－Ⅱ在车辆动态监控/调度实验平台中的应用[J]. 电子测量技术，2007(10)：146－149.

[3] Labrosse J. 嵌入式实时操作系统 μC/OS－Ⅱ[M]. 邵贝贝等，译. 北京：北京航空航天大学出版社，2003：245－269.

[4] 吴国民. μC/OS－Ⅱ实现实时消息传递[J]. 现代计算机：专业版，2007(10)：132－134.

[5] 周世杰，刘锦德，秦志光. 消息队列技术研究：综述与一个实例[J]. 计算机科学，2002(2)：84－86.

[6] 朱方娥，曹宝香. 基于 JMS 的消息队列中间件的研究与实现[J]. 计算机技术与发展，2008，18(5)：172－175.

[7] Tai Stefan. Conditional Messaging: Extending Reliable Messaging with Application Conditions[C]//Proceedings of the 22nd International Conference on Distributed Computing Systems. [s.l.]:[s.n.],2002:123－132.

[8] Chiang Mei－Ling, Li Yun－Chen. LyraNET: A zero－copy TCP/IP protocol stack for embedded operating systems[C]// 11th IEEE International Embedded and Real－Time Computing Systems and Applications. [s.l.]:[s.n.], 2005: 123－128.

(上接第 150 页)

on Security and Privacy. Oakland, CA:[s.n.],1999.

[4] Bass T. Intrusion detection systems and multisensor data fusion[J]. Communications of the ACM, 2000, 43(4): 99－105.

[5] Giacinto G, Roli F, Didaci L. Fusion of multiple classifiers for intrusion detection in computer networks[J]. Pattern Recognition Letters, 2003, 24(12): 1795－1803.

[6] 郭文普，孙继银. 一种基于数据融合的分布式入侵检测系统[J]. 计算机技术与发展，2006，16(2)：217－219.

[7] Lippmann R P, Cunningham R K. Improving intrusion detection performance using keyword selection and neural networks [J]. Computer Networks, 2000, 34(4): 597－603.

[8] Ghosh A K, Schwartzbard A. A Study in Using Neural Networks for Anomaly and Misuse Detection [C]//The 3rd USENIX Windows NT Symposium. Seattle, Washington: [s.n.],1999.

[9] 李之堂，李家春. 模糊神经网络在入侵检测中的应用[J]. 小型微型计算机系统，2002，23(10)：1235－1238.

[10] Stolfo S J, Fan Wei, Lee Wenke, et al. Task description of Kddcup'99[EB/OL]. 1999. http://kdd.ics.uci.edu/databases/kddcup99/task.html.