基于改进神经网络的网络入侵检测

刘 建
(东莞理工学校,广东 东莞 523000)

摘 要:随着计算机网络的高速发展,从 20 世纪 90 年代初至今的几十年中,网络安全问题日渐突出,计算机信息的安全和防御受到严重影响。传统非神经网络入侵检测包含着效率低、误差较大和收敛速度慢等问题。采用改进的遗传算法来使神经网络权值与 BP 算法结合,能够满足入侵检测分类识别的需求,利用给定的动态神经网络系统构建相应的网络入侵检测系统,能适应不同类型的入侵检测,有效地提高了网络的安全性。

关键词:改进神经网络;网络入侵检测;遗传算法
中图分类号:TP393.08 文献标志码:A 文章编号:2095-2945(2018)02-0011-03

Abstract: With the rapid development of computer network, in the past decades from the beginning of the 1990s to the present, the problem of network security has become increasingly prominent, and the security and defense of computer information have been seriously affected. Traditional non-neural network intrusion detection includes problems such as low efficiency, large error and slow convergence rate. The improved genetic algorithm is used to combine the weights of neural network with BP algorithm, which can meet the needs of intrusion detection classification and recognition, and construct the corresponding network intrusion detection system using the given dynamic neural network system. This adapts to different types of intrusion detection and effectively improves the security of the network.

Keywords: improved neural network; network intrusion detection; genetic algorithm

引言

社会信息化进程不断提高的今天,在享受计算机带来的众多便利时,网络安全问题也不容忽视[1]。被动的网络入侵检测和防御机制已经无法满足现在网络的需求,基于改进神经网络的动态化网络入侵检测,在信息爆炸的时代中,日益成为网络安全领域的重要技术手段。传统基于规则的入侵检测技术在管理和建模上存在一些问题,基于改进神经网络的入侵检测,利用神经网络模糊的运算能力,可以一定程度上解决模式识别中的问题。网络入侵检测是对网络上的数据进行识别,将其分类为正常或者非正常的数据。传统的 BP 神经网络本身存在着算法的限制,容易陷入数值局部最小,利用改进的遗传算法优化神经网络权值,一定程度上加强全局数据搜索能力,提高系统实用性。研究神经网络系统的相关原理和基于改进神经网络的入侵检测系统的优点,设计将神经网络应用于网络检测,能够使改进的遗传算法更适合于入侵监测系统。

1 神经网络和网络入侵检测流程

神经网络是对人脑的简单抽象与模拟,它包含多重简单单元组成的并行网络,模拟人的神经系统对世界做出交互反应。神经网络将信息的存储与处理之间的界限消除,介入到网络检测领域,为一些问题的提出提供了新的思路[2]。神经网络不同于传统的只用一个计算单元计算的模式,系统采集大量的数据为系统提供样本,通过不断的学习建立计算模型,继而建立神经网络计算模型,它的基本功能是通过交互神经元的大规模并行运算实现。

人们对入侵检测系统的研究应用,使传统网络安全技术的不足被更多的关注,网络入侵检测系统的逐步完善,将为网络安全提供更多的保障。入侵检测技术是网络安全系统中的一个重要环节,在安全监测中,能够发现网络系统中的安全漏洞,安全检测工具可以实现实时动态对网络系统攻击的监测,通过监测和分析用户的系统活动,检查系统存在的漏洞,关注数据文件的完整性来识别攻击行为,统计异常行为的同时识别用户活动中违反安全的部分。它的工作原理实际上就是从不同的环节收集和分析信息,记录并报告检测结果的过程。如图 1 所示:

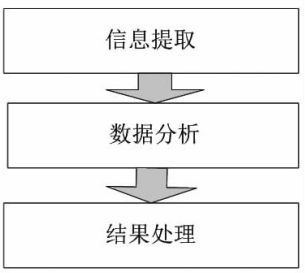

图 1 网络入侵检测过程图

一般来说,网络入侵检测系统的组成构件主要包括数据源、从数据源收集数据的传感器、行为、分析处理收集到数据的分析器、事件、管理器和响应器等。将神经网络应用于网络入侵检测,提供系统的审计数据给神经网络,它就可以提取到用户与系统的正常特征模式。神经网络在了解入侵实例后就可以对新的攻击模式产生反应,使网络入侵检测具有主动性,

作者简介:刘建(1979-),男,汉族,广东东莞人,软件工程硕士,计算机讲师,主要研究方向:计算机。

同时反应出偏离系统正常工作的事件[3]。随着网络攻击手段的发展，网络入侵技术的发展也有了新的要求，更好的将神经网络应用于网络入侵检测，改进神经网络和入侵检测，是我们研究的重要内容。

2 基于改进神经网络的网络入侵检测设计

神经网络在解决模式识别问题时存在怎样选择结构和参数的问题，虽然神经网络具有强大的能力，但是为了提供更加的性能，改进神经网络为一种可调节的动态神经网络是非常有价值的开发工作。这种入侵检测系统的原理是从网络中捕捉数据，数据包进行提取信息并解析，特征提取模块得到的属性送入系统，最后由 GABP 检测引擎进行辨别。GABP 检测引擎模块的设计的原理是，先训练 BP 神经网络，再经由 GA 优化复制、交叉，直到训练过程达到标准，这种优化带来的局部最小值，使学习效率得到了提高，保证了入侵检测系统的准确程度。改进后的网络入侵检测系统的神经网络结构如图 2 所示：

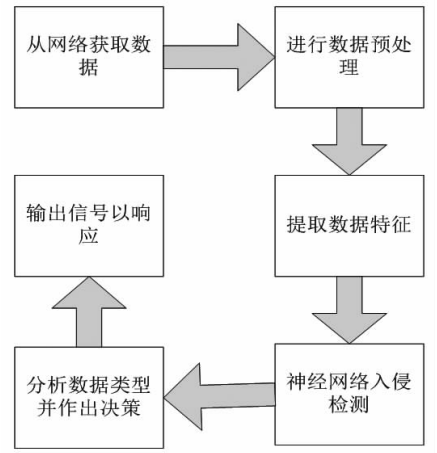

图 2 基于改进神经网络的网络入侵检测结构

神经网络中输入与输出的关系函数通常定义为

$$E=\frac{1}{2}(D-O)^2 \quad (1)$$

公式中 $D=(d_1,\cdots,d_l)$ 为期望输出，$O=(o_1,\cdots,o_l)$ 为实际输出。在本网络入侵检测系统中，数据采集是进行数据检查和做出决策的基础条件，网络信息采集包的准确性和可靠性直接影响监测系统的工作效率，数据尽量完整，才能实现对系统检测攻击能力的提升。基于改进神经网络的入侵检测模型主要包含获取网络信息的数据模块、预处理信息的数据模块、提取特征的模块、神经网络入侵检测的模块等[4]。要实现这种模型就要通过 Packet Capture library 访问数据链路层，与 Snort 软件相结合，将收集到的数据转化为 ASCII 字符信息，利用脚本语言编写处理程序来获得信息中的基本属性，对比不同连接模式中的频繁模式指导特征提取；将挖掘出的复杂数据属性进行降维处理，标定适应度值，放大个体适应度，选择操作前保留当前最优解，适应度函数值的计算为：

$$f(x)=\frac{1}{\sum_{i=1}^{n}(t-t_i)^2} \quad (2)$$

公式中 t 是预测值，t_i 是真实值，n 为样本数，以局部改进的 GABP 算法训练神经网络，用与最大适应函数相对的权值计算，防止陷入局部极小值。

网络入侵检测作为主动防卫系统安全的技术，需要在攻击技术不断出现的未知攻击中，将改进神经网络作为研究热点[5]。神经算法中最常见的是 Back Propagation 神经网络，为了克服它存在的缺点，建立遗传算法优化的 BP 神经网络入侵检测系统模型将发挥神经网络的泛化映射能力。改进算法将综合增加动量与自适应调节学习速率相结合，可以调整网络学习速率，因此要先建立 BP 神经网络模型。这个过程包括：确定输入和输出、隐层层数的节点个数；调整并确立网络参数，开始训练神经网络；趋于稳定时在训练次数达到规定的要求时结束训练学习，此时如果神经网络的评测结果达到准确程度，BP 网络模型就建立好了。

3 仿真实验

入侵检测技术已经取得了较快的发展，我们能够检测网络攻击的状况，通过截取网络数据包数据的方式，实现验证基于 BP 神经网络的入侵检测模型的准确程度实验采用 Lincoln 实验室数据作为网络入侵检测模型测试的数据集，将 Matlab R2007 作为仿真平台，用相关的神经网络函数对实验数据进行调用。实验的 CPU 为 AMD Athlon XP 1700+，采用 SQL 2000 Server 数据库。在 IDS 系统的测试环境中，通过不同类型的攻击进行训练和测试，验证本网络入侵系统检测模型的检测能力和检查率。实验的步骤包括：(1) 使用 600 个样本作为网络训练的依据，150 个样本作为进行测试的依据，通过检验比较出改进后的算法与传统神经网络的检测差别，对数据的特征进行编码，以 Premnmx() 函数归一数据在一定区间内。(2) 确定神经网络的结构，参考理论与实验，将网络拓扑确定为 8–10–1，网格训练的最大次数为 3000，隐含层与输出层的激励函数为双曲函数和线性函数。(3) 采用 BP 神经网络和改进的方法进行测试，初始值取值范围为–0.3~0.3.学习误差为 0.0001，输入节点为 50，隐含节点为 60，输出节点为 1。利用遗传算法对自变量进行优化选择。(4) 筛选出最优解以优化改进神经网络，将筛选后的变量作为改进后神经网络的输入，将结构改变为新的内容。

将选取的数据结果进行分析，实验中采取的经 PCA 技术预处理的数据，在降低数据维数的同时，大大缩短了神经网络的测试时间。对比着传统的神经网络，改进后的网络不仅收敛速度快，还具有更高的检测率和正确性。试验检测结果如图 3 所示。

由上图可以看到，改进后的网络入侵检测系统相比传统的网络入侵检测模型具有更高的检测率，能够有效地提高网络的安全性。改进神经网络的识别率能够达到 96%以上，在检测入侵上具有巨大的发展潜力，在优化遗传算法自变量之后，加快的收敛速度能有效地缩短时间，显著提高了检测率。

4 结束语

通过本文的研究可以发现，依据传统神经网络的特点。将改进后的神经网络应用于网络入侵检测中，优化筛选参与

（下转 14 页）

为了验证所建立模型以及参数辨识结果，需建立该模型的离散方程，利用 Hppc 实验数据进行仿真验证。

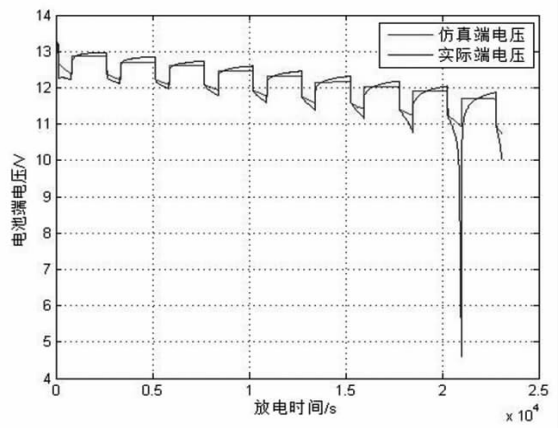

图 2 电池端电压 U_L 仿真结果

以实测回路电流 i 为输入变量，电池荷电状态 SOC、极化电压 U_{p1}、U_{p2} 为状态转移变量，电池端电压 U_L 为输出变量，建立方程如下：

$$\begin{pmatrix} SOC_{k+1} \\ U_{p1k+1} \\ U_{p2k+1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{-\Delta t/\tau_1} & 0 \\ 0 & 0 & e^{-\Delta t/\tau_2} \end{pmatrix} \begin{pmatrix} SOC_k \\ U_{p1k} \\ U_{p2k} \end{pmatrix} + \begin{pmatrix} -\frac{\Delta t}{Q} \\ R_{p1}\left(1-e^{-\Delta t/\tau_1}\right) \\ R_{p2}\left(1-e^{-\Delta t/\tau_2}\right) \end{pmatrix} i_k \quad (2)$$

$$U_{Lk} = U_{OCV} - i_k R_0 - U_{p1k} - U_{p2k} \quad (3)$$

其中 U_{OCV}、R_0、R_{p1}、R_{p2}、C_{p1}、C_{p2} 均为关于 SOC 的可变参数。在 Matlab 中进行编程仿真以上的离散方程，以 Hppc 实验实测的 I_L 作为输入，得到仿真结果如图 2 所示。

分析仿真结果可以看出，仿真电池端电压波形能基本与实际电池端电压波形拟合，但是在电池放电及电池端电压恢复的暂态过程仍存在一定误差，这可能是由于暂态参数 R_{p1}、R_{p2}、C_{p1}、C_{p2} 的辨识存在一定误差所导致的。同时，该模型并不能模拟深度放电时电池端电压骤降的过程。但总体而言，改进 PNGV 模型仍可以在电池正常工作状态下较好地体现出电池的特性。

4 结束语

本章在建立了改进 PNGV 模型，建立离散数学模型模拟 Hppc 实验过程，代入各可变参数进行仿真，由仿真结果证明了在电池常规工作状态下，该模型能够较好的体现出电池的特性。

参考文献：

[1]杨新法，苏剑，吕志鹏，等.微电网技术综述[J].中国电机工程学报，2014(1)：57–70.
[2]张娟.铅酸电池储能系统建模与应用研究[D].湖南大学，2013.
[3]邓磊.基于改进 PNGV 模型的动力锂电池 SOC 估计和充电优化[D].哈尔滨工业大学，2014.
[4]欧阳佳佳.储能电池管理系统研究[D].浙江大学，2016.
[5]Haihua Zhou，Bhattacharya T，Duong Tran，et al. Composite Energy Storage System Involving Battery and Ultracapacitor With Dynamic Energy Management in Microgrid Applications [J]. IEEE Transactions on Power Electronics，2011，26(3)：923–930.
[6]Peng Z，Hui Li，Gui–Jia Su，Lawler S. A new ZVS bidirectional DC –DC converter for fuel cell and battery application [J].IEEE Transactions on Power Electronics，2004，19(1)：54–65.
[7]Y Nozaki，K Akiyama，H Kawaguchi，et al. An improved method for controlling an EDLC–battery hybrid stand–alone photo–voltaic power system[C]. IEEE APEC，2000：781–786.
[8]徐杰.基于卡尔曼滤波的动力电池组 SOC 精确估计[D].杭州电子科技大学，2009.
[9]王标.基于电池模型的汽车铅酸电池 SOC 在线估计方法研究[D].合肥工业大学，2015.
[10]谢广.基于无迹卡尔曼滤波的磷酸铁锂电池 soc 估算研究[D].合肥工业大学，2015.

(上接 12 页)

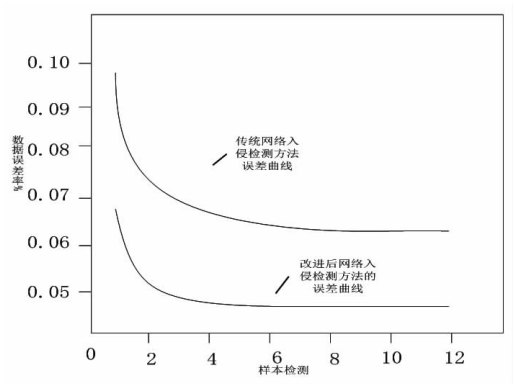

图 3 仿真结果误差率的比较与分析

建模的自变量，能有效地减少误差，提高效率缩短时间。网络入侵检测是全新的具备主动性的安全防护技术，基于改进神经网络的入侵检测成为网络安全技术提升必不可少的补充。随着网络规模的扩大和手段的变化，网络入侵检测能力也提出了更高的要求[6]。传统 BP 神经网络模型限制了网络入侵检测系统的应用，改进后的神经网络在网络入侵检测中的应用能力和研究成果还需要进一步的深入，争取构建网络入侵检测与身份认证、数据加密等技术相结合的多层次防护体系。

参考文献：

[1]罗俊松.基于神经网络的 BP 算法研究及在网络入侵检测中的应用[J].现代电子技术，2017，40(11)：91–94.
[2]詹沐清.神经网络技术在网络入侵检测模型及系统中的应用[J].现代电子技术，2015，38(21)：105–108.
[3]周立军，张杰，吕海燕.基于数据挖掘技术的网络入侵检测技术研究[J].现代电子技术，2016，39(6)：10–13.
[4]张永良，张智勤，吴鸿韬，等.基于改进卷积神经网络的周界入侵检测方法[J].计算机科学，2017，44(3)：182–186.
[5]刘浩然，赵翠香，李轩，等.一种基于改进遗传算法的神经网络优化算法研究[J].仪器仪表学报，2016，37(7)：1573–1580.
[6]刘敬，谷利泽，钮心忻，等.基于神经网络和遗传算法的网络安全事件分析方法[J].北京邮电大学学报，2015，38(2)：50–54.