靠性和安全性，在各学校网络边界处部署防火墙，防止外部用户非法访问各学校的内网，同时可以建立在教委出口防火墙和各学校出口防火墙之间的安全连接，传输私密数据。

基于 BP 神经网络的网络安全态势预测

◆杨武俊

（运城学院数学与信息技术学院　山西　044000）

摘要：网络的普及使人们时时刻刻都在接触互联网。计算机网络进入了全新的时代，同时网络攻击和网络安全问题也日益严重。借助 BP 神经网络良好的预测精度和非线性泛化能力，建立基于 BP 神经网络的网络安全态势预测模型，通过实验数据，实现对网络安全态势演变趋势的预测，最终为保障互联网安全提供有效的数据保障。

关键词：P 神经网络；安全态势；权重；指标体系

基金项目：全国高等院校计算机基础教育研究会，计算机基础粗教育教学研究项目（2019-AFCEC-345）

随着物联网、云计算、大数据的快速发展，计算机网络进入了高速发展的时代，人们已经习惯了互联网提供的各种服务。与此同时，计算机网络面临着巨大的风险，如网络攻击、网络金融诈骗、密码窃取、病毒侵入等。随着网络服务的不断普及，我国公民的个人信息和重要数据保护非常不足，信息泄露的形势极为严峻，针对出现的种种网络安全问题，网络安全态势感知逐渐成为预测和防范网络安全问题的焦点，网络安全态势感知技术被广泛研究和应用。

BP神经网络具有较强的自学习能力和处理非线性问题能力[1]，由于网络安全态势预测所涉及的既有定量的指标又有定性的指标，所以建立态势预测与影响网络安全因素之间关系的神经网络模型，能够很好将影响网络安全的各种指标因素统一起来，建立适合网络安全态势预测的模型[2]。对预测结果进行分析，找出影响网络安全的各种不同因素，及各种因素所造成的网络危害的严重程度，对网络安全进行有针对性的主动安全防护和预防。

1　网络安全态势评估体系

1.1 网络安全态势

态势感知是指在一定时间和空间范围内动态、整体地洞悉安全风险的能力。将状态信息与已知标签进行对比，进而得出当前网络的安全运行情况[3]。随着互联网的兴起，而发展升级为“网络态势感知”。

网络态势感知是指在具体的网络环境下，对影响网络安全的要素进行提取，综合各方面的安全要素，从整体上反映网络的安全状况。态势感知能够全面感知网络安全的威胁、洞悉网络的应用运行状态、通过全面的分析，实现网络攻击的实时评估，帮助管理人员采取针对性响应处置措施，确保网络安全[4]。

安全态势预测是整个态势感知模型中最顶层的应用技术。网络安全态势的预测对网络安全的防御有着重要的作用，态势预测的定义是对未来将要发生的事件或场景进行预先的估计来判定其发生可能性的大小[5]。

1.2 网络安全态势预测指标体系建立

在对网络安全态势进行预测时，为保证实际的处理效果，需要构建完整的态势感知的指标体系，保证数据的采集，预处理，以此指标体系为基础，通过 BP 神经网络算法，进行态势感知预测。目前，对于企业网络安全态势预测，应用的指标体系包括一级指标[6]（U_i）：1、恶意程序，2、安全漏洞，3、服务攻击，4、网站安全，5、云平台安全，6、互联网金融安全等方面。及对应的二级指标（u_{ij}）。如下表 1 所示。

表 1 安全态势预测内容及指标

一级指标（U_i）	二级指标（u_{ij}）
恶意程序（U_1）	1. 计算机恶意程序 2. 移动互联网恶意程序 3. 联网智能设备恶意程序
安全漏洞（U_2）	1. 应用程序漏洞 2. Web 应用漏洞 3. 操作系统漏洞 4. 网络设备漏洞 5. 数据库漏洞 6. 安全产品漏洞
服务攻击（U_3）	1. 网站攻击 2. 数据库攻击 3. 邮箱攻击
网站安全（U_4）	1. 仿冒网页 2. 网站后门 3. 网页篡改
云平台安全（U_5）	1. 云平台攻击 2. 数据泄露
互联网金融安全（U_6）	1. 网络 APP 攻击 2. 明文传送 3. 网络支付交易

2　基于 BP 神经网络的安全态势预测

2.1　BP 神经网络算法

神经网络（NN）是基于模仿生物神经网络结构和功能而建立的一种信息处理系统。BP网络采用多层结构，包括输入层、隐含层和输出层，隐含层可以是多层[7]。各层通过全连接进行连接，每一层内的神经元之间不存在连接关系[8]。一般是采用具有一个输入层、一个隐含层和一个输出层的三层网络模型结构[9]。三层BP神经网络中，输入层 $X=(x_1,x_2,\cdots x_n)$，隐含层 $H=(h_1,h_2\cdots h_t)$，输出层 $Y=(y_1,y_2\cdots y_m)$。

2.2 基于 BP 算法的神经网络安全态势预测的结构设计

（1）输入层。选取数据，作为输入层的输入数据。根据上表建立的预测指标体系，对网络安全态势预测的网络输入包括影响网络安全的20项参数（见表1），因此输入层的节点数为20。输入向量 $=(x_1,x_2,\cdots x_{20})$，当各分量物理意义相同且为同一量纲时，应在整个数据范围内确定最大值和最小值，然后进行同一的变换处理，以使输入的评价目标值在区间[0,1]中[10]。针对指标的不同量级，对数据进行归一化处理公式如下：

$$x_i=\frac{x_i-x_{min}}{x_{max}-x_{min}} \quad (1)$$

（2）隐含层。对于隐含层节点个数的设置，在本实验中，先设置 10 个节点，再进行不断的训练，通过误差分析来逐步增减隐含层的神经元数目，直至得到满意的性能。计算公式如下[11]：

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

$$h_j = f(\sum_{i=0}^{n} W_{ij}\, x_i) \quad (2)$$

W_{ij} 表示节点 i 和节点 j 之间的权值，首先随机化权值的大小，取（-1，1）之间的随机数，通过训练调整权值的大小。

（3）输出层。输出层节点数为标签个数，神经元的传递函数用非线性变换函数 Sigmoid 函数。计算公式如下：

$$S(x) = \frac{1}{1+e^{-x}} \quad (3)$$

通过函数 S(x)的计算，得出各个输出节点的值，数值为[0,1]之间的数，通过概率的大小对网络安全进行预测。数值越大，受网络攻击就越大。对于网络的安全就要加大防范。

3　实验仿真

本次实验选取了某公司 12 月份的网络数据日志进行分析，包括 3 台服务器，10 台主机，总共有 500 个样本点数据，选取其中的 400 个样本点数据，进行神经网络训练，对参数进行拟合调整。剩余 100 个样本点，进行网络的安全预测。在训练中，学习率取 0.02，各层的权值首先随机输入，根据训练目标进行调整，训练以预测值与标签的均方误差 MSE<=0.003，当均方误差达到要求时，训练结束，神经网络的参数随之确定，用训练好的神经网络参数对剩余 100 个样本点进行预测。训练用 Anaconda 语言中的神经网络模型实现训练模型。选取 100 个样本点中的部分时段网络安全态势预测值为表 2 所示。

表 2 网络安全态势预测结果

编号	标签	编号	标签	编号	标签
1	0.967	7	0.843	13	0.465
2	0.857	8	0.891	14	0.671
3	0.754	9	0.175	15	0.748
4	0.384	10	0.266	16	0.639
5	0.965	11	0.833	17	0.683
6	0.432	12	0.785	18	0.974

对于表2中的预测结果，根据网络安全的分层结果可知，对于像编号1的值0.967，编号5的值0.965，编号18的值0.974都是网络安全危害非常大，存在很大漏洞，需要加强防范。对于像编号9中的值0.175，数值较小，可知在这一时段网络安全，对网络的攻击，漏洞都很小。数值越小，网络越安全。

4　结语

本文通过设置影响网络安全态势的指标，提出了一种基于 BP 神经网络安全态势预测的模型。通过实验仿真，能够很好对网络安全进行预测，使预测结果更加精准，能很好拟合网络安全情况，提供安全防护的理论根据，指导网络管理者可以及时发现网络中的安全威胁和漏洞，更好地做好防护，实现主动防御。

参考文献：

[1]孟磊，于庆锋，宋永超.人工神经网络方法（BP）在变形监测中的应用[J].测绘与空间地理信息，2018，41（7）：215-218.

[2]Bass T，Gruber D.A glimpse into the future of id[J]. The Magazine of Usenix&Sage，1999，24（3）：40-49.

[3]Endsley M. Design and evaluation for situation awareness enhancement[C]//Proc of the Human Factors society Annual Meeting.Los Angeles，CA：SAGE Publications，1988：97-101.

[4]李馥娟，王群.网络安全态势感知实训平台设计与实践[J].实验技术与管理，2020，37（4）：124-128.

[5]肖喜生，龙春，彭凯飞等. 基于人工智能的安全态势预测技术研究综述[J].信息安全研究，2020（6）：505-513

[6]中华人民共和国国家互联网信息办公室. 2019 年上半年我国互联网网络安全态势[EB/OL].2019[2019-8-13]. http://www.cac.gov.cn/2019-08/13/c_1124871484.htm.

[7]焦李成. 神经网络系统理论[M]. 西安：西安电子科技大学出版社，1990.

[8]吴简彤，王建华. 神经网络技术及其应用[M]. 哈尔滨：哈尔滨工程大学出版社，1998.

[9]林仕高，欧元贤. BP 神经网络学习参数优化研究[J]. 微计算机信息，2010.

[10]柳小桐. BP 神经网络输入层数据归一化研究[J]. 机械工程与自动化，2010（03）：122-123+126.

[11]常江华.BP 神经网络算法在智能钻进控制系统中的应用[J].煤矿机械，2020，41（05）：188-191.

基于 Docker 容器虚拟化技术的 WordPress 系统研究

◆周少珂　吴华芹　谢妞妞　付媛冰

（河南应用技术职业学院　河南　450042）

摘要：随着计算机硬件技术发展，由依靠数量的增加以提高其运行效率的横向传统发展模式，逐步向提高硬件利用率支持虚拟化的纵向发展模式。根据应用虚拟化技术的基础架构不同，分为软件虚拟化和硬件虚拟化两类。首先针对基于 Docker 容器的 Linux 开源操作系统的软件虚拟化技术进行研究；然后在 Linux 系统平台上搭建能够资源隔离的 Docker 容器，并在该容器中搭建和配置 WordPress 博客项目系统；最后通过使用 Docker 容器模式与传统模式的系统进行对比，表明使用该 Docker 容器虚拟化模式架设的系统更加高效、稳定，为 Docker 虚拟化的进一步应用研究做好准备。

关键词：云计算；虚拟化；容器；Docker；Linux

基金项目：河南省教育科学“十三五”规划课题（2020YB0499）；河南应用技术职业学院校级科技类项目（2019B-KJ-17）

1　Docker 容器配置

随着计算机硬件技术的发展，各项硬件技术指标都得到了巨大提高，但单纯地提高各项硬件指标，已无法满足人们对工作效率的需求。虚拟化技术的产生和发展，进一步提升各个硬件设备工作中的并发量，能够进一步提高现有的硬件资源利用率[1]。

虚拟化技术是计算机资源管理技术的一种，通过一定的技术手段将底层的硬件资源如 CPU、内存、硬盘、网络等设备，按照一定组织方式进行抽取、组合，打破传统之间的隔离、物理硬件之间不可切割的障碍，使用户按比原本更加合理的方式，利用逻辑组织硬件资源的技术[2]。根据作用对象不同可分为：硬件虚拟化和软件虚拟化；根

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net