PCA-BP神经网络入侵检测方法

梁 辰， 李成海， 周来恩
(空军工程大学防空反导学院,西安,710051)

摘要 针对经典BP神经网络在入侵检测应用中收敛速度慢、学习性能不够理想等缺陷,以消除原始数据中的冗余信息、提升入侵检测算法的检测性能为目的,综合采用主成分分析法和附加动量法,提出了一种基于PCA-BP神经网络的入侵检测方法,通过对数据的特征选择和对网络的权值修正,对经典BP神经网络算法进行了拓展和改进。首先对网络数据集进行标准化处理,并对处理后的数据集进行降维处理以确定主分量的特征数,最后将处理完成后的数据集输入到改进的BP神经网络中进行检测。通过在KDD Cup 1999网络数据集上的大量实验证明,该方法在大部分网络环境,尤其是在训练样本较为充足的网络环境中时,系统模型的收敛性、检测效率和检测准确率上均优于经典BP神经网络方法和半监督入侵检测方法。

关键词 入侵检测系统;主成分分析;BP神经网络;附加动量法;入侵检测算法
DOI 10.3969/j.issn.1009-3516.2016.06.017
中图分类号 TP393.08 **文献标志码** A **文章编号** 1009-3516(2016)06-0093-06

A PCA-BP Neural Network-based Intrusion Detection Method

LIANG Chen, LI Chenghai, ZHOU Laien
(Air & Missile Defense College, Air Force Engineering University, Xi'an 710051, China)

Abstract: Aimed at the problems that slow convergence speed, poor learning performance and other imperfections exist in the classical BP neural network intrusion detection, a PCA-BP neural network intrusion detection method is put forward by adopting principal components analysis and additional momentum method, This method improves the classical BP neural network algorithm by data features selection and network weights amendment. Firstly, the paper standardizes the network data set, and then adopts it to deal with dimension reduction to confirm the characteristics. Finally, the paper detects the processed data set by improved BP neural network. Through the lots of experiments in KDD Cup 1999 network data sets, the result shows that the method has better performances in system model convergence, detection efficiency and detection accuracy in most network environment. Especially, in training samples, the convergence of system model, the detection efficiency and the detection accuracy are better than that by using BP neural network algorithm and half-supervision intrusion detection algorithm.

Key words: intrusion detection system; principle component analysis; back propagation neural network; additional momentum; intrusion detection algorithm

收稿日期:2016-01-06
基金项目:国家自然科学基金(61309022)
作者简介:梁 辰(1992—),男,湖北十堰人,硕士生,主要从事网络信息安全研究.E-mail:3659442@qq.com

引用格式:*梁辰,李成海,周来恩.PCA-BP神经网络入侵检测方法[J].空军工程大学学报:自然科学版,2016,17(6):93-98. LIANG Chen, LI Chenghai, ZHOU Laien. A PCA-BP Neural Network-based Intrusion Detection Method[J]. Journal of Air Force Engineering University: Natural Science Edition, 2016, 17(6): 93-98.*

入侵检测(Intrusion Detection)是一种动态的网络安全技术,它建立在入侵行为与系统行为不同这一假设基础上,通过分析网络流量或系统审计记录等,实时发现网络或系统中是否有违反安全策略的攻击行为,对可能危害到系统机密性、完整性和可用性的行为进行响应和拦截[1]。

自 1987 年 D.E.Denning[2] 提出入侵检测的概念至今,入侵检测技术引起了各界广泛关注,各种基于机器学习的入侵检测方法被应用到该领域中,如 Lee[3] 提出的基于数据挖掘技术的检测方法,从审计数据或数据流中提取感兴趣的知识,并用这些知识去检测异常入侵和已知的入侵,这种方法可以适应处理大量数据的情况,但并不能高效地进行实时入侵检测;郑黎明[4] 提出的基于支持向量机的入侵检测方法,解决了入侵检测系统先验知识较少情况下推广能力差的问题,使得入侵检测系统在小样本的条件下仍然具有良好的推广能力,但是当输入数据集很大时,SVM 方法的计算速度也会下降较大,且单纯的支持向量机对于多元问题的处理仍没有很好的解决办法;李元兵[5] 提出的基于神经网络的检测方法,使得入侵检测系统在识别未知攻击方面具有更好的性能。

传统的入侵检测系统对网络入侵的检测效率低,占用资源高,其中有些不能及时防御突发入侵事件,有些不能识别未知或变化的网络攻击行为,在有效性、灵活性和响应能力等方面都有一定的局限性。而基于神经网络的入侵检测系统具有高度的自学习和自适应的能力,神经网络可以不断地学习更新,对网络中的数据信息进行更准确的分析和处理,从而达到识别入侵信息的目的[6]。

综合上述对入侵检测方法的研究,本文提出了一种基于 PCA-BP 神经网络的入侵检测方法。文中将主成分分析(Principal Component Analysis, PCA)方法和用附加动量法改进的 BP 神经网络方法相结合,并采用 KDD Cup 1999 网络入侵检测数据集[7] 对本文提出的方法模型进行训练和测试。

1 相关工作

人工神经网络由神经元模型构成,这种由许多神经元组成的信息处理网络具有并行处理和大规模平行计算能力,能高度逼近非线性系统,并对不确定问题具有自我学习能力[8]。而 BP 神经网络及它的变化或改进形式是目前实际应用中使用最广泛的网络模型,它是前向网络的核心部分,是人工神经网络的精华之所在。

PCA 方法和 BP 神经网络方法均可单独应用在入侵检测系统中。但是,PCA 方法不能有效捕捉入侵数据各种因素之间的非线性关系,不能直接用于建立入侵检测系统模型。BP 神经网络方法可以直接用于入侵检测系统模型的建立,但由于入侵检测数据需要考虑的影响因素较多,如果不经处理将所有影响因素输入 BP 神经网络,将会使得神经网络收敛速度缓慢,泛化能力较差。

本文以提高算法收敛性能为目的,对 BP 算法进行了适当的改进。先对原始入侵检测数据中的重叠信息进行处理,再将由 PCA 获得的主成分信息送入 BP 神经网络的输入层进行训练。网络拓扑结构见图 1。这种方法在能够发挥 BP 神经网络的非线性建模能力的基础上,简化了数据输入,提高了系统的鲁棒性和泛化能力[9]。

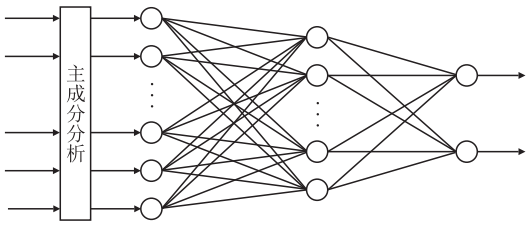

图 1 PCA-BP 神经网络拓扑结构图

Fig.1 Topological structure of PCA-BP neural network

2 基于 PCA-BP 神经网络的入侵检测算法

入侵检测算法是入侵检测系统的核心。在对相关网络数据的分析中得知,系统要处理的数据大多都是高维数据,且彼此存在着一定的相关性,数据在一定程度上反映的信息有所重叠。为改进神经网络的性能,构造更稳定的入侵检测核心算法,本文在采用主成分分析法对相关网络数据进行降维处理的基础上,使用附加动量法对经典的 BP 神经网络方法进行改进[10],并应用在入侵检测中。

2.1 主成分分析

主成分分析(Principal Component Analysis, PCA)或者主元分析是一种掌握事物主要矛盾(主要特征)的多元统计分析方法[11]。PCA 方法最早由 Karl Parson 于 1901 年对非随机变量引入,它利用降维的思想,对于原始的所有变量建立尽可能少的两两不相关的新变量,并使这些变量能反映原变量的绝大部分信息,且所含的信息互不重叠。这些新变量称为原始变量的主成分。

PCA 在保证能尽可能多的反映原始入侵数据信息的基础上，压缩原有数据集的规模，将入侵检测数据集进行简化。步骤如下：

1）设原始数据集 X 有 m 个数据，每个数据有 p 个特征属性，即 $\boldsymbol{X}=(\boldsymbol{X}_1,\boldsymbol{X}_2,...,\boldsymbol{X}_m)^{\mathrm{T}}$，$\boldsymbol{X}_i=(x_{i1},x_{i2},...,x_{ip})$（$i=1,2,...,m$），其中 T 表示向量的转置。将原始数据矩阵 $\boldsymbol{X}$ 标准化：$X_m\times p^*=\dfrac{\boldsymbol{X}-\mathrm{mean}(\boldsymbol{X})}{\sqrt{\mathrm{std}(\boldsymbol{X})}}$，并计算 $\boldsymbol{X}^*_{m\times p}$ 的协方差矩阵 $\boldsymbol{Y}_{p\times p}$；

2）通过特征方程 $(\lambda\boldsymbol{I}-\boldsymbol{Y})\boldsymbol{\alpha}=0$，求得协方差矩阵 $\boldsymbol{Y}_{p\times p}$ 的各特征值 λ_i（从小到大顺序排列）和对应的特征向量 $\boldsymbol{\alpha}_i$（$i=1,2,...,p$）

3）计算主成分贡献率及累计贡献率：

主成分为：

$$Z_i=\boldsymbol{\alpha}_i\times\boldsymbol{X}^*_{m\times p}(i=1,2,...,p)\tag{1}$$

Z_i 的贡献率为：

$$\frac{\lambda_i}{\sum_{i=1}^{p}\lambda_i}(i=1,2,...,p)\tag{2}$$

主成分的累计贡献率为：

$$\frac{\sum_{i=1}^{k}\lambda_i}{\sum_{i=1}^{p}\lambda_i}(i=1,2,...,p)\tag{3}$$

4）这里选取参数 k，取得主成分 $Z_1,Z_2,...,Z_k(k\leqslant p)$，分析对象由 p 维降为 k 维。

2.2　改进的 BP 神经网络算法

2.2.1　经典 BP 神经网络算法

经典的 BP 算法基于梯度下降法，由正向传播和反向传播组成。在正向传播过程中，输入信息从输入层经隐含层单元逐层处理后，传至输出层。在逐层处理的过程中，每一层神经元的状态只影响下一层神经元的状态。若现行输出不等于期望输出，则进入反向传播，把误差信号沿原连接路径返回，通过计算目标函数对网络权值和阈值的梯度进行修正，直到误差信号最小[12]。

神经网络中各节点的传递函数为 Sigmoid 函数 $f(x)=\dfrac{1}{1+e^{-x}}$。

经典的反向传播公式如下：

$$\boldsymbol{f}(k+1)=\boldsymbol{f}(\boldsymbol{k})-r\,\nabla F(\boldsymbol{f}(k))\tag{4}$$

式中：$\boldsymbol{f}(k)$ 为网络所有权值和阈值形成的向量；r 为学习速率；$F(\boldsymbol{f}(k))$ 为目标函数；$\nabla F(\boldsymbol{f}(k))$ 为目标函数的梯度；k 为迭代次数。

2.2.2　附加动量法

为了解决网络在误差曲面上变化趋势的影响，平滑网络训练收敛曲线的震荡，在每次学习的权值改变时利用本次训练和上一次训练的权值变化[13]。其权值修正的迭代过程为[14]：

$$\boldsymbol{f}(k+1)=\lambda(\boldsymbol{f}(k)-\boldsymbol{f}(k-1))+(1-\lambda)r\,\nabla F(f(k)))\ (0\leqslant\lambda\leqslant1)\tag{5}$$

当动量因子 λ 取 0 时，权值的变化就是由经典的反向传播算法产生的；当动量因子 λ 取 1 时，新的权值变化等于上一次权值的变化，忽略了梯度下降方法产生的变化部分。

2.3　算法说明

基于 PCA-BP 神经网络的入侵检测算法的描述如下：

输入：网络数据集 L、U，并且网络数据 x 满足 $x\in U$。

输出：网络数据 x 的类型。

1）将网络数据集 L 按 2.1 中方法降维至某个确定特征维数 $k(k=1,2,...,40)$，得到处理后的数据集 L'；

2）以处理后的网络数据集 L' 为训练集输入到改进的 BP 神经网络中，训练入侵检测模型；

3）输入网络数据集 U 作为测试集，其中每一个网络数据 x 满足 $x\in U$；

4）判断网络数据 x 的类型。

算法模型见图 2。

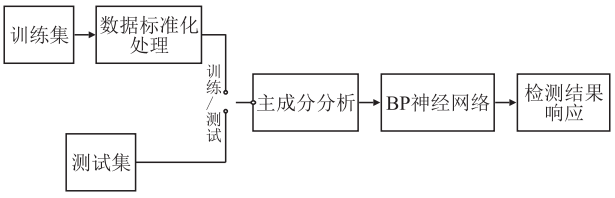

图 2　基于 PCA-BP 神经网络算法的入侵检测模型

Fig.2　Model of PCA-BP neural network-based intrusion detection algorithm

3　实验

入侵检测实验采用 KDD CUP 1999 数据集在 Matlab R2014a 平台上进行。

3.1　数据描述

由于 KDD 数据集过于庞大，实验中选用 8 类共 32 000 条数据组成训练数据集，其中正常数据 20 000条，7 类攻击数据共计 12 000 条，每类数据中有标记数据所占比例为 3%，另选用包含训练数据集中 8 种数据类型的 19 000 条数据作为测试数据集。所用数据集见表 1。

表 1 KDD CUP99 10%数据集攻击行为及分布

Tab.1 Aggression and distribution of KDD CUP99 10% data set

数据类型 Data Type	数量	
	训练数据集 Training Data	测试数据集 Test Data
normal(0)	20 000	10 000
smurf(1)	3 000	2 000
satan(2)	1 500	1 000
portsweep(3)	1 000	1 000
neptune(4)	3 000	2 000
back(5)	1 500	1 000
ipsweep(6)	1 000	1 000
warezclient(7)	1 000	1 000
Total	32 000	19 000

3.2 标准化处理

数据集中一条网络连接记录共包含 41 个属性特征,其中 3 个为符号型变量,其余为数值型变量。由于不同的属性特征有不同的度量标准,在进行检测时,首先对抽取出来的数据集中数据的属性特征进行标准化处理。首先,采用按 TCP 连接基本特征类型区分的方式把 3 个符号型变量转换成数值型变量。如在协议类型属性有 TCP、ICMP、UDP3 种类型,分别将其置为 1、2、3。然后将所有的数值型变量进行标准化处理:

首先计算数据集数据样本第 j 个分量的均值 $\overline{x_j}$ 和它的标准差 s_j,即:

$$\overline{x_j}=\frac{1}{n}\sum_{i=1}^{n}x_{ij},\ s_j=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_{ij}-\overline{x_j})} \tag{6}$$

式中:n 为数据集中的样本数,再对第 j 个属性特征进行标准化变化,有 $\overline{x_j}'=\frac{(x_{ij}-\overline{x_j})}{s_j}x_{ij}$ 为训练集第 i 个样本的第 j 个分量。

3.3 模型检测

首先,通过一系列实验,确定文中所述入侵检测模型中的相关参数(主分量特征数目、隐含层神经元数目)。采用 3.1 中所述训练数据集 L 和测试数据集 U,以 3.2 节所述方法对其进行标准化处理后,将训练集 L 进行降维,以确定主分量的特征数目 k($k=1,2,\cdots,40$)。处理完成后输入到改进的 BP 神经网络中。取隐含层神经元个数为 i($i=1,2,\ldots,50$)。最后,使用测试数据集 U,通过基于 PCA-BP 神经网络的入侵检测方法进行判别。

重复取包含 3.1 节中所述训练测试集所有的 8 种类型的网络数据集进行多次实验。

进行对比分析得知,主成分数目达到 28 个时主成分信息基本可以完全反映原始数据信息。同时隐藏神经元数目小于 10 个时分类器性能较差,大于 45 个时易形成过拟合现象。综上所述,当主成分数目为 28 个,隐藏神经元数目为 39 个时,神经网络的入侵检测准确率和收敛性能最优。不同参数下入侵检测算法的的检测准确率见表 2。

表 2 不同参数下入侵检测准确率对比

Tab.2 Comparison of detection rate in different parameters

隐藏神经元数目 \ 主成分数目	10	15	20	25	28	30	35	40
10	0.765 18	0.778 62	0.812 62	0.895 88	0.935 61	0.938 00	0.950 40	0.964 20
20	0.745 16	0.801 60	0.807 50	0.909 52	0.964 80	0.994 60	0.995 81	0.994 28
25	0.742 64	0.734 56	0.734 62	0.756 04	0.976 61	0.996 00	0.995 00	0.994 07
30	0.742 42	0.806 68	0.753 46	0.898 66	0.986 04	0.996 50	0.994 83	0.995 40
35	0.751 64	0.803 20	0.831 44	0.807 92	0.996 40	0.996 60	0.994 49	0.994 80
39	0.775 60	0.759 34	0.937 08	0.952 84	0.996 60	0.995 64	0.995 86	0.995 67
40	0.751 64	0.742 56	0.803 10	0.800 66	0.995 45	0.996 03	0.995 40	0.996 00
45	0.742 80	0.742 56	0.944 02	0.746 06	0.995 22	0.996 04	0.995 44	0.985 00
50	0.749 14	0.751 30	0.896 42	0.914 72	0.956 26	0.965 80	0.967 00	0.985 23

3.4 对比实验

表 3 列出了在相同实验条件下 PCA-BP 神经网络算法、经典 BP 神经网络算法、和半监督 GHSOM 算法[15]的检测率情况。其中,PCA-BP 神经网络算法,主分量特征维度取 29,隐藏神经元数目取 39。

通过对比可以看出,相对于经典的 BP 神经网络算法,采用 PCA-BP 算法后,总体检测率由 68.22%提高到 88.2%。多数类型(normal,satan,ipsweep,portsweep,back)的检测率均有不同程度的提高,其中对 ipsweep,satan 类型的检测率提高较大。少数类型(smurf,Neptune)的检测率变化不明显;个别类型(warezclient)的检测率有所下降,原因是经典的 BP 算法对该攻击类型数据的检测率本来就很低(0.564%),在 PCA-BP 算法训练过程中,一部分表征数据特征值在进行主成分分析的过程中因为权值过小被忽略了,导致极少数量的该类型数据在检测中被误判。从以上分析得知,PCA-BP 算法对那些使用经典 BP 神经网络算法获得一定检测

率且有较大改进空间的攻击类型具有较好的改进效果；对那些原本已具有较高检测率的攻击类型，改进效果不明显；对原有检测率较低的个别攻击类型，可能会有一定的负面影响。总体上，相对于经典的 BP 神经网络算法，PCA-BP 算法明显具有更好的检测性能。

表 3　各算法分类准确率对比

Tab.3　Comparison of detection rate of different algorithms

数据类型	正确检测到的数据个数			准确率		
	BP	Semi-Supervised GHSOM	PCA-BP	BP	Semi-Supervised GHSOM	PCA-BP
normal	6 395	9 261	9 291	0.639 5	0.926 1	0.929 1
smurf	2 000	2 000	2 000	1.000 0	1.000 0	1.000 0
satan	571	832	840	0.571 0	0.832 0	0.840 0
portsweep	713	787	810	0.713 0	0.787 0	0.810 0
Neptune	1 583	1 734	1 732	0.791 5	0.867 0	0.866 0
back	698	833	868	0.698 0	0.833 0	0.868 0
ipsweep	437	641	675	0.437 0	0.641 0	0.675 0
warezclient	564	423	542	0.564 0	0.423 0	0.542 0
Total	12 961	16 511	16 758	0.682 2	0.869 0	0.882 0

相对于半监督的 GHSOM 算法，PCA-BP 算法在入侵检测中检测率均略有提高，在 warezclient 类型的检测率上提升较为明显。原因是在半监督 GHSOM 算法中，前期落在某些神经元上的 warezclient 类型的数据数量较无监督增多，后期大量与 warezclient 特征较为类似的 normal 类型数据落在这些神经元上将 warezclient 类型的数据淹没掉，导致该神经元所代表的类型被认为是 normal 类型，从而使得检测过程中会有更多的 warezclient 类型的数据被误判为 normal 类型，而 PCA-BP 算法作为无监督算法则不存在这样的问题[16]。但同时也注意到，半监督的 GHSOM 算法在训练样本不足的网络环境中具有更好的实用性。综上可知，PCA-BP 算法在大部分网络环境中具有更高的实用性和更优的算法复杂度[17]。

4　结语

本文在将 PCA 方法和 BP 神经网络相结合的基础上，使用附加动量法对 BP 算法进行了适当的改进，提出了一种新的入侵检测算法。实验证明，这种方法在能够发挥 BP 神经网络的学习能力和适应性的基础上，简化了数据输入，因此，具有更好的检测效率。

文中所提出的方法在具体应用中还需要根据实际情况作进一步的改进，以提高其稳定性和性能[18]。如何更合理确定主成分特征数目、隐含层神经元数目以及如何将本文所述的方法应用于实际的网络环境中将是我们下一步的工作重点。

参考文献(References)：

[1] CHANDOLA Varun, BANERJEE Arindam, KUMAR Vipin. Anomaly Detection: a Survey [J]. ACM Computing Surveys, 2009, 41(3): 15:1-15:58.

[2] DENNING D E. An Intrusion Detection Model[J]. IEEE Transactions on Software Engineering, 1987, SE-13: 222-232.

[3] STOLFO S, LEE W. Data Mining Approaches for Intrusion Detection[R]. New York: Columbia Univ New York Dept of Computer Science, 2000.

[4] 郑黎明，邹鹏，贾焰. 多维多层次网络流量异常检测研究[J]. 计算机研究与发展，2011，48(8)：1506-1516.
ZHENG Liming, ZOU Peng, JIA Yan. Anomaly Detection Using Multi-Level and Multi-Dimensional Analyzing of Network Traffic[J]. Journal of Computer Research and Development, 2011, 48(8): 1506-1516.(in Chinese)

[5] 李元兵，房鼎益，吴晓南. 基于神经网络的异常入侵检测系统[J]. 系统工程与电子技术，2005，27(9)：1648-1651.
LI Yuanbing, FANG Dingyi, WU Xiaonan. Anomaly Intrusion Detection System Based on Neural Network [J]. Systems Engineering and Electronics. 2005, 27(9): 1648-1651.(in Chinese)

[6] 李晨光. 基于神经网络的入侵检测技术研究与应用[D].长春：吉林大学，2013.
LI Chenguang. Research and Application of Network Intrusion Detection Technique Based on Neural Networks[D].Changchun: Jilin University, 2013.(in Chinese)

[7] The UCI KDD Archive. KDD99 Cup Dataset[DB/OL].(1999-10-28)[2015-11-11].http://kdd.ics.uci.edu/databases/kddcup99/ kddcup99.html.

[8] Tsungnan Lin, Chiapin Wang, Po-Chiang Lin. A Neural-Network-Based Context-Aware Handoff Algorithm for Multimedia Computing[J]. ACM Transactions on Multimedia Computing, Communications, and Applications,2008, 4(3):17:1-17:23.

[9] 徐立鹏, 葛良全, 谷懿. 基于 PCA-BP 神经网络的 EDXRF 分析测定地质样品中铁、钛元素含量的应用研究[J]. 光谱学与光谱分析,2013, 33(5): 1392-1396.
XU Lipeng, GE Liangquan, GU Yi. Research on the Application of Principal Component Analysis and Improved BP Neural Network to the Determination of Fe and Ti Contents in Geological Samples[J]. Spectroscopy and Spectral Analysis,2013, 33(5): 1392-1396.(in Chinese)

[10] TIAN Jingwen, GAO Meijuan. Network Intrusion Detection Method Based on High Speed and Precise Algorithm Neural Network[C]//Proc of International Conference on Networks Security, Wireless Communications and Trusted Computing. 2009: 619-622.

[11] CAMACHO Jose,FERRER Alberto.Cross-Validation in Pca Models with the Element-Wise K-Fold(Ekf) Algorithm: Practical Aspects[J]. Chemometrics and Intelligent Laboratory Systems,2014, 131: 37-50.

[12] 丁士圻. 人工神经网络基础[M]. 哈尔滨: 哈尔滨工程大学出版社, 2008.
DING Shiqi. Basis of Artificial Neural Network[M]. Harbin: Harbin Engineering University Press, 2008.

[13] ZHENG Dezhi, PENG Peng, FAN Shangchun. A Research of Dynamic Compensation of Coriolis Mass Flowmeter Based on BP Neural Networks[J]. Instruments and Experimental Techniques, 2013, 56(3): 365-370.

[14] 刘慧, 余艳梅, 罗代升. 基于动量 BP 神经网络的英文字符识别[J]. 四川大学学报:自然科学版,2011, 48(6): 1324-1326.
LIU Hui, YU YanMei, LUO DaiSheng. English Character Recognition Based on Momentum BP Neural Network[J]. Journal of Sichuan University:Natural Science Edition,2011, 48(6): 1324-1326.(in Chinese)

[15] 阳时来, 杨雅辉, 沈晴霓,等. 一种基于半监督 GHSOM 的入侵检测方法[J]. 计算机研究与发展,2013, 20(11): 2375-2382.
YANG Shilai, YANG Yahui, SHEN Qingni. A Method of Intrusion Detection Based on Semi-Supervised GHSOM[J]. Journal of Computer Research and Development,2013, 20(11): 2375-2382.(in Chinese)

[16] 杨雅辉, 黄海珍, 沈晴霓. 基于增量式 GHSOM 神经网络模型的入侵检测研究[J]. 计算机学报,2014, 37(11):1216-1224.
YANG Yahui,HUANG Haizhen, SHEN Qingni. Research on Intrusion Detection Based on Incremental GHSOM[J]. Chinese Journal of Computers,2014, 37(11):1216-1224.(in Chinese).

[17] 杨雅辉. 网络流量异常检测及分析的研究[J]. 计算机科学,2008, 35(5): 108-112.
YANG Yahui. Research on Anomaly Detection and Analysis Based on Network Traffic[J]. Computer Science,2008, 35(5): 108-112.(in Chinese)

[18] 范晓诗,雷英杰,王亚男. 流量异常检测中的直觉模糊推理方法 [J]. 电子与信息学报,2015, 37(9):2218-2224.
FAN Xiaoshi, LEI Yingjie, WANG Yanan. Intuitionistic Fuzzy Reasoning Method in Traffic Anomaly Detection[J]. Journal of Electronics & Information Technology,2015, 37(9):2218-2224.(in Chinese)

(编辑:徐楠楠)