

# 免疫算法优化的 RBF 在入侵检测中的应用

曹耀彬,王亚刚

(西安邮电大学 计算机学院,陕西 西安 710121)

**摘要:** RBF(Radical Basis Function)神经网络是一种典型的三层前向神经网络。虽然 RBF 神经网络的非线性逼近能力、分类能力以及学习速度都要好于其他的神经网络,但是 RBF 神经网络在实际应用中隐含层中心点难求,不能被广泛地应用于入侵检测系统中。免疫算法是基于免疫系统的学习算法,免疫算法不仅对干扰具有较强维持系统平衡的能力,而且具有较强的模式分类能力。为了得到最优的 RBF 神经网络并将其应用到入侵检测系统中,提出了一种免疫算法优化的基于最小均方差的联合 RBF 神经网络,即 IA-LMS-RBF 算法。仿真实验结果表明,与传统的  $K$ -means 和随机法选取基函数中心点相比,基于免疫算法求取中心点的 LMS-RBF 神经网络,不仅能明显地提高对已知攻击的检测能力,并且对于未知的攻击行为也能很好地进行识别。IA-LMS-RBF 算法有效提高了入侵检测系统的效率,保证了计算机系统的安全性。

**关键词:** 入侵检测;RBF 神经网络;中心点;  $K$ -means;免疫算法;最小均方差

**中图分类号:** TP301.6

**文献标识码:** A

**文章编号:** 1673-629X(2017)06-0114-05

doi:10.3969/j.issn.1673-629X.2017.06.024

## Application of RBF Neural Network Optimized by Immune Algorithm in Intrusion Detection

CAO Yao-bin, WANG Ya-gang

(College of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

**Abstract:** RBF neural network is a typical three-layer feed forward neural network. Although approximation capacity, classification and learning speed of RBF neural network is superior to others, it is difficult to find the optimal value of the center point which is not used widely in intrusion detection system. Immune algorithm is a learning algorithm based on the immune system. It not only owns a strong ability to maintain system balance, but also has strong pattern classification. In order to get the optimal RBF neural network and apply it to the intrusion detection system, an immune algorithm has been proposed to optimize the LMS-RBF neural network, which is based on the minimum mean square, called as associated IA-LMS-RBF algorithm. Simulation results shows that compared with the traditional  $K$ -means and randomly to select the basis function center, the immune algorithm to strike the center of the LMS-RBF neural network not only significantly improves the ability to detect the known attacks, but also has a good recognition to the unknown attacks, IA-LMS-RBF algorithm can effectively improve the efficiency of intrusion detection system and make sure computer system is becoming more secure.

**Key words:** intrusion detection; RBF neural network; center point;  $K$ -means; immune algorithm; LMS

## 1 概述

入侵检测系统<sup>[1-2]</sup> (Intrusion Detection System, IDS)指的是用来对各种入侵行为进行检测的系统,是网络安全体系的重要组成部分,通过对网络和计算机系统的运行状态进行监视,发现各种攻击企图,然后及时发出报警并做出相应的反应,以保证系统资源的机密性、完整性与可用性。

入侵检测的分析方法主要包括误用检测和异常检测。误用检测是根据已知的入侵模式来检测系统中的

入侵行为,误用检测会提取已知的各种攻击的行为特征,然后编写为入侵模式存储到异常行为数据库中,如果入侵者的行为正好与数据库中的某个模式匹配就判断为攻击。误用检测具有较高的检测率和较低的误报率,其缺点是一般只能检测到已知攻击模型,而对未知的攻击行为不敏感<sup>[3-4]</sup>。而异常检测恰恰相反,异常检测会提取已知的用户的正常行为特征,并存储到正常行为数据库中,如果用户的行为和正常行为数据库中的模式偏差太大,就判别为攻击,所以异常检测的误

收稿日期:2016-06-12

修回日期:2016-09-22

网络出版时间:2017-03-13

基金项目:国家自然科学基金资助项目(61136002);陕西省教育科研计划项目(14JK1674)

作者简介:曹耀彬(1990-),男,硕士生,研究方向为网络安全;王亚刚,博士,副教授,CCF 会员,研究方向为嵌入式系统、编译器与并行计算。

网络出版地址: <http://jns.cnki.net/kcms/detail/61.1450.TP.20170313.1547.092.html>

报率较高。

为了解决上述两个问题,目前已有很多先进技术应用于 IDS 中。文献[5]采用基于模糊 C 均值与决策树 C4.5 的双过滤机制,充分发挥模糊 C 均值对未知攻击的检测能力和 C4.5 的低误报率。针对传统 BP 神经网络存在容易陷入局部最优、收敛速度慢等缺点,文献[6]提出了人工蜂群优化的 BP 神经网络在入侵检测中的应用,文献[7]提出将粒子群优化的 BP 神经网络应用到入侵检测中。针对支持向量机,文献[8]提出了网格搜索优化支持向量机参数的入侵检测系统。

鉴于 RBF 神经网络的许多优点,可以将其应用到入侵检测中,但是其隐含层基函数的参数(宽度、中心点与数量)对网络的性能有很大影响。目前传统的 RBF 神经网络采用聚类或者随机的方法确定 RBF 神经网络的中心点,不过由于隐含层的基函数是非线性的,文献[9]充分描述了采用这些方法确定径向基神经网络中心点的位置与数量,不仅会造成局部极小值的出现,而且网络的收敛速度也会放慢,造成网络资源的浪费,从而降低 RBF 神经网络的性能。该文献初步描述并证明了采用免疫类方法求取径向基神经网络中心点位置与数量的可能性及其优点。

针对这一问题,文中提出了一种基于免疫算法与最小均方差(Least Mean Square, LMS)算法<sup>[10]</sup>的混合训练算法。该算法使用免疫算法计算隐含层基函数的中心点,并利用 LMS 算法对连接权值做进一步的学习,求解隐含层到输出层的权值矩阵,这样得到的 RBF 神经网络模型具有较高的泛化能力。

## 2 RBF 神经网络

1985 年, Powell M. J. D 提出多变量插值的径向基函数,其方法在某种程度上利用了多维空间中传统的严格插值法的研究成果。20 世纪 80 年代末, J. Moody 和 C. Darken 提出了 RBF 神经网络。RBF 神经网络模拟了人脑中局部调整、相互覆盖接受域的神经网络结构,因此是一种局部逼近网络,现已证明它能以任意的精度逼近任意连续函数。

RBF 神经网络是一种三层前馈神经网络,其不同于多层感知器,不同层有着不同的功能,其结构如图 1 所示。

第一层为输入层,由感知器组成,其作用主要是将网络和外部的环境连接起来;第二层为非线性的隐含层,采用径向基函数将输入层的数据映射到更高维的隐含层,使原来线性不可分的问题变得线性可分;第三层为输出层,负责将隐含层的数据组合输出。

对于一个  $p$  维的输入向量, RBF 神经网络的输入

可用式(1)计算。

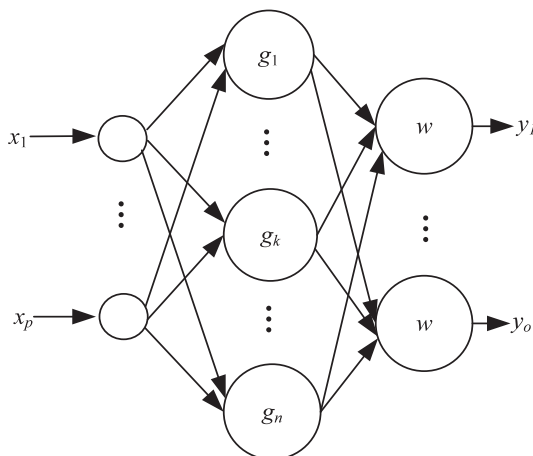


图1 RBF神经网络结构

$$y_o = \sum_{i=1}^n w_{ij} \exp\left(-\frac{1}{2\sigma^2} \|x_i^p - c_i\|^2\right) \quad (1)$$

其中,  $x_i^p = (x_1^p, x_2^p, \dots, x_m^p)$  为第  $i$  ( $i = 1, 2, \dots, m, m$  为样本总数) 个输入样本;  $c_i$  为网络隐含层节点的中心;  $w_{ij}$  ( $j = 1, 2, \dots, n, n$  为隐含层节点数) 为隐含层到输出层的权值矩阵;  $y_o$  为与输入样本对应的第  $o$  个输出节点的实际输出。

因为 RBF 神经网络的输出为线性神经元,因此只要确定了隐含层基函数的三个参数,就能通过线性优化方法构造出隐含层到输出的权值矩阵。因此 RBF 学习算法的主要任务是确定隐含层的这三个参数,其中传统的隐含层中心点的确定方法有无监督的聚类算法(如  $K$ -means<sup>[11]</sup>)与随机选取法,但是这两种方法都需要事先人为指定中心点,很难得到全局最优值。

## 3 免疫算法

免疫算法(Immune Algorithm, IA)是一种基于生物免疫系统的进化算法,它模拟了免疫系统独有的学习、记忆、识别等功能,主要借鉴免疫学中的克隆选择学说<sup>[12]</sup>和免疫网络理论<sup>[13]</sup>。其中克隆选择学说解释了免疫系统是如何响应抗原入侵的,免疫网络理论说明了抗原、抗体与记忆细胞(抗原的映射)之间的相互作用关系。

### 3.1 免疫原理

在免疫系统中,抗原-抗体相互作用的强度用它们的亲和力表示。设第  $i$  个输入数据  $x_i$  与第  $j$  个数据中心  $c_j$  之间的亲和力为  $a_{ij}$ ,即

$$a_{ij} = \frac{1}{1 + \|x_i - c_j\|} \quad (2)$$

其中,  $\|x_i - c_j\|$  为  $x_i$  与  $c_j$  之间的欧氏距离。当  $x_i = c_j$  时,  $a_{ij} = 1$  为最大。

而抗体与抗体之间的相互作用由它们的相似度来描述:设第  $i$  个数据中心  $c_i$  与第  $j$  个数据中心  $c_j$  之间的

相似度为  $s_{ij}$ , 即

$$s_{ij} = \frac{1}{1 + \|c_i - c_j\|} \quad (3)$$

其中,  $\|c_i - c_j\|$  为  $c_i$  与  $c_j$  之间的欧氏距离。当  $c_i = c_j$  时,  $s_{ij} = 1$  为最大。

假设  $n$  个输入数据  $x = [x_1, x_2, \dots, x_n]$ , 每个输入  $x_i = [x_{i1}, x_{i2}, \dots, x_{id}]$ ,  $i = 1, 2, \dots, n$ 。确定 RBF 的中心就是要寻找一个新的数据集  $c = [c_1, c_2, \dots, c_j]$ , 其中  $c_j = [c_{j1}, c_{j2}, \dots, c_{jd}]$ ,  $j = 1, 2, \dots, m, m < n$ 。

### 3.2 算法步骤

基于 IA 的 RBF 神经网络隐含层基函数的中心点确定主要分为三个步骤: 随机选择一个中心点集合, 中心点的个数与位置无关紧要; 应用克隆选择理论控制数据中心点的选择与更新; 采用免疫网络理论确认并消除那些自我识别的中心点, 控制中心点的数量。算法的具体步骤如下:

(1) 对于每一个输入数据  $x_i$ , 随机初始化  $C$  中心点数据集, 包含所有可选的中心点。

(2) 计算  $C$  中所有可选的中心点与  $x_i$  的亲合力  $a_{ij}$ , 选择  $n$  个亲合力最大的中心点并进行复制,  $a_{ij}$  越大, 复制得越多, 此时产生一个中心点数量为  $m$  的复制集合  $L$ 。

(3) 应用式(4)对这  $m$  个相同的中心点进行变异处理, 形成变异集合  $D$ ,  $\beta_k$  为变异率。这一过程实际上是在有最大亲和力的中心点附近搜索更具亲和力的数据中心。

$$c_k = c_k - \beta_k(c_k - x_i) \quad (4)$$

(4) 重新计算  $x_i$  与  $D$  中每个中心点之间的亲合力, 并选择出  $\% \xi$  (为成熟抗体细胞, 即中心点数量的选择比例) 亲合力最大的中心点, 创建记忆细胞的集合  $M_i$ 。

(5) 在  $M_i$  中删除那些相似度大于阈值  $\sigma_1$  (表示免疫细胞自然死亡阈值) 的中心点, 获得一个压缩的  $M_s$ 。

(6) 计算  $M_s$  中各记忆细胞之间的相似度  $s_{ij}$ , 除去那些相似度小于阈值  $\sigma_2$  (表示抑制阈值) 的网络中心点, 这一过程体现了免疫系统中的克隆抑制, 然后将  $M_s$  合并到  $M$ 。

(7) 所有的输入  $x_i$  处理完后, 计算  $M$  中各中心点的相似度  $s_{ij}$ , 删除掉相似度小于  $\sigma_2$  的中心点, 这一步体现了遗传算法中的网络抑制。

(8) 用新的中心点替换  $C$  中亲合力较低的数据中心, 这些新增加的数据中心可以随机选取, 这一过程体现了免疫系统的自组织性。

(9) 判断  $C$  中心点集合是否不再变化, 若成立则整个确定中心点的递推过程结束,  $C$  即为所求的 RBF 中

心点集合。

(10) 否则判断递推步数是否达到预定步数, 若达到则整个递推过程结束,  $C$  即为所求的 RBF 中心点集合, 若没有则转向步骤(2)。

## 4 LMS 算法

对于 RBF 神经网络, 采用固定径向基函数作为隐含层的训练函数, 采用标准差固定的高斯函数作为隐含层的基函数:

$$g(\|x_i - c_j\|, \sigma_j) = \exp\left(-\frac{\|x_i - c_j\|^2}{\sigma_j^2}\right) \quad (5)$$

$$\sigma_j = d_{\max} / \sqrt{2m_1} \quad (6)$$

其中,  $j = 1, 2, \dots, m_1$ , 为隐含层中心点的个数;  $d_{\max}$  为中心点之间的最大距离;  $x_i$  为输入数据;  $c_j$  为第  $j$  个中心点;  $\sigma_j$  的选择必须保证径向基函数不能太尖或太平。

通过 IA 求得隐含层基函数的中心点以及标准差后, 学习过程的下一步就是采用 LMS 算法来训练 RBF 神经网络, 其中网络的目标函数为:

$$E = \frac{1}{2} \sum_{j=1}^N e_j^2 \quad (7)$$

$$e_j = d_j - \sum_{i=1}^{m_1} w_i(n) g(\|x_j - c_j(n)\|) \quad (8)$$

式(9)为 LMS 算法的权值矩阵修正公式。

$$w_i(n+1) = w_i(n) + \eta \sum_{j=1}^N e_j g(\|x_j - c_j(n)\|) \quad (9)$$

式(10)为 LMS 算法的隐含层中心点修正公式。

$$c_j(n+1) = c_j(n) + \eta \frac{\partial E(n)}{\partial c_j(n)} \quad (10)$$

式(11)为 LMS 算法的标准差修正公式。

$$\sigma_j^{-1}(n+1) = \sigma_j^{-1}(n) + \eta \frac{\partial E(n)}{\partial \sigma_j^{-1}(n)} \quad (11)$$

其中,  $c_j(n)$  为径向基函数在第  $n$  次迭代时的第  $j$  个中心点;  $x_j$  为第  $j$  个训练样本;  $d_j$  为第  $j$  个训练样本的期望输出;  $\eta$  为学习率。

## 5 IA-LMS-RBF 算法

如图 2 所示, 基于 IA-LMS-RBF 算法的入侵检测系统主要分为两个部分。第一部分(虚线箭头)利用从 KDD CUP 数据集中选取的训练数据对基于 IA 求取中心点的 RBF 神经网络采用 LMS 算法进行训练, 求取全局最优参数。第二部分(实线箭头)利用从 KDD CUP 数据集中选取的测试数据, 对参数确定的 RBF 神经网络模型进行测试, 判断测试的数据是否为入侵行为, 其主要步骤如下:

- (1)将随机初始化的中心点送入 IA 算法中,即采用 3.2 节的算法步骤求取全局最优的中心点集合。
- (2)应用式(6)计算 RBF 标准差。
- (3)用小的随机数初始化权值矩阵。
- (4)对于每一个训练数据  $x_i$ ,应用式(1)计算 RBF 神经网络的相应输出  $y_i$ 。
- (5)应用 LMS 算法对训练样本进行训练,即按式(9)~(11)调整权值矩阵、中心点位置与标准差。如果网络收敛则停止迭代,否则转向步骤(4)继续迭代,如果迭代次数超过预定值大小,则停止。
- (6)对于每一个测试数据  $x_j$ ,应用式(1)计算输出,判断测试结果。

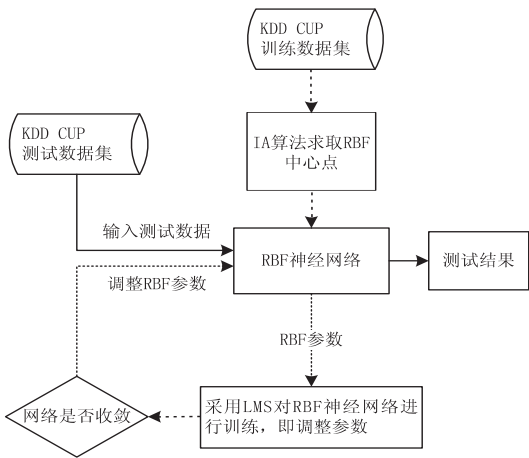


图2 IA-LMS-RBF 入侵检测流程图

6 实验

6.1 数据预处理

实验数据采用 KDD CUP 99 数据集<sup>[14]</sup>(是由美国麻省理工学院林肯实验室提供),通常采用该数据集对设计的 IDS 模型进行各种性能测试。其中所有数据都是在实际运行的互联网环境下模拟真实攻击的情景得到的,该数据集大约有 500 万条数据,39 种攻击类型,每一条数据由 42 个属性值组成,前 41 个属性表示其特征,唯一标识一条数据,第 42 个属性标识该数据是正常行为产生的,还是入侵行为产生的,数据样例如下:

0,tcp,http,SF,241,1857,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,13,13,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,255,1.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,normal

0,udp,private,SF,105,147,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,2,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,254,1.00,0.01,0.00,0.00,0.00,0.00,0.00,0.00,0.00,normal

该数据集的 42 个属性值中有数值型属性,也有非

数值型属性,因为 RBF 算法不能处理文字,所以这里需要对数据进行归一化处理,即用数值型的数据代替基于符号串的数据,其中需要修改的有数据的第 2、3、4 和 42 维共四种:

协议类型(protocol\_type)编码:tcp 编码 1,udp 编码 2,icmp 编码 3。

目标主机的网络服务(service)类型:因为网络服务类型一共有 70 种,所以这里使用数字 1~70 分别对其进行编码。

连接正常或错误的状态(flag),离散类型,共 11 种:OTH REJ RSTO RSTOS0 RSTR S0 S1 S2 S3 SF SH,用数字 1~11 对其进行编码。

KDD CUP 99 数据集中每条连接记录的第 42 个属性标识了这条数据攻击类型,具体可以分为五大类:Normal DOS Probing R2L U2R,分别用数字 1~5 对其进行标识。

6.2 实验设计

为了评价入侵检测算法的性能,选取了入侵检测性能好坏的两个标准:检测率和误报率。

检测率=(检测出的入侵样本数/入侵样本总数)\*100%

误报率=(被误报为入侵行为的正常样本数/正常样本总数)\*100%

实验选用 10% KDD CUP 99 数据集,其中包含 494 021 条数据。不过其中 normal 与 DOS 类型的数据太多,大约占了数据总数的 99% 左右,如果将该数据集作为训练样本,重复太多,浪费了训练时间,所以在这里对这两种数据按比例删减,使数据分布更加合理。表 1 为原始数据与删减后数据的数量对比。

表1 数据集的删减

分类	normal	DOS	probing	R2L	U2R
原始	97 278	391 458	4 107	1 126	52
删减	4 229	17 019	4 107	1 126	52

将删减后数据集中的每种攻击类型的数据按 1:2:3:1 的比例分成四组,其中前三组数据作为训练数据,第四组数据作为测试样本,然后再从 corrected 数据集<sup>[14]</sup>中选取 1 000 条未知类型的攻击行为作为第五组数据,用于测试模型对于未知类型攻击的敏感程度。

6.3 实验仿真

分别采用随机法、基于 K-means 和基于免疫算法选取中心点的 RBF 神经网络的入侵检测系统模型进行仿真实验,主要测试了系统对于正常数据的误报率、对已知类型的攻击行为的检测率和对未知类型的攻击行为的敏感程度。使用三组训练样本分别训练模型



后,对两组测试样本的测试结果见表 2~4。

表 2 随机选取法的测试结果 %

训练样本	检测率(已知)	误检率	检测率(未知)
3 788	68.55	30.24	40.48
7 576	72.39	26.22	59.21
11 364	81.51	14.89	65.00

表 3 基于  $K$ -means 算法的测试结果 %

训练样本	检测率(已知)	误检率	检测率(未知)
3 788	74.45	23.77	53.22
7 576	75.34	18.93	57.91
11 364	90.29	12.79	69.33

表 4 基于免疫算法的测试结果 %

训练样本	检测率(已知)	误检率	检测率(未知)
3 788	78.51	11.26	70.76
7 576	86.43	8.19	89.27
11 364	95.33	5.72	96.19

从表中可以明显看出,随着训练样本数的提高,准确率也相应提高。随机选取法和  $K$ -means 对未知类型攻击的检测率要比已知类型攻击的检测率平均低 20% 左右,而基于 IA 选取中心点的 RBF 对未知类型的攻击与已知类型的攻击的检测率基本一致,所以和传统的中心点确定方法相比,基于免疫算法的 RBF 神经网络入侵检测模型不论是整体检测能力,还是对未知攻击类型的泛化能力都要好于其他两种,由此可见 IA 能够选取最优中心点优化 RBF 神经网络。

7 结束语

针对 RBF 神经网络中基函数的中心点及其数量很难确定这一问题,探讨了传统的  $K$ -means 和随机法选取 RBF 神经网络基函数中心点的不足,提出了基于免疫算法优化的采用最小均方差训练的 RBF 神经网络并将其应用到入侵检测系统中。仿真实验结果表明,启发式的免疫算法求取 RBF 神经网络隐含层基函数的中心点即 IA-LMS-RBF 算法,与原有算法相比,提高了入侵检测系统的检测率,降低了误检率,使入侵

检测系统对于未知攻击类型的入侵行为更加敏感,更加优化了入侵检测系统的性能。

参考文献:

[1] Stalling W, Brown L. Computer security principles and practice[M]. 2nd ed. America: Pearson Education, Inc., 2012.

[2] 李文明,陈哲,李绪蓉. 缓存区溢出研究与发展[J]. 计算机应用研究,2014,31(9):2651-2566.

[3] Kim G, Lee S, Kim S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection[J]. Expert Systems with Applications, 2014, 41(4):1690-1700.

[4] Park N H, Oh S H, Lee W S. Anomaly intrusion detection by clustering transactional audit streams in a host computer[J]. Information Sciences, 2010, 180(12):2375-2389.

[5] 滕少华,严远驰,刘冬宁,等. 基于 FCM-C4.5 的双过滤入侵检测机制[J]. 计算机应用与软件, 2016, 33(1):307-311.

[6] 沈夏炯,王龙,韩道军. 人工蜂群优化的 BP 神经网络在入侵检测中的应用[J]. 计算机工程, 2016, 42(2):190-194.

[7] 傅德胜,张媛. PSO 优化 BP 神经网络入侵检测模型[J]. 通信技术, 2010, 43(1):81-83.

[8] 张公让,万飞. 基于网格搜索的 SVM 在入侵检测中的应用[J]. 计算机技术与发展, 2016, 26(1):97-100.

[9] Nunes L, Zuben F J V. An immunological approach to initialize centers of radical basis function neural networks[C]// Proceedings of V Brazilian conference on neural network. [s. l.]:[s. n.], 2001.

[10] 林嘉宇,刘荧. RBF 神经网络的梯度下降训练方法中的学习步长优化[J]. 信号处理, 2002, 18(1):43-48.

[11] 刘华春,候向宁,杨忠. 基于改进 K 均值算法的入侵检测系统设计[J]. 计算机技术与发展, 2016, 26(1):101-105.

[12] Brownlee J. A review of the clonal selection theory of acquired immunity[R]. [s. l.]:[s. n.], 2007.

[13] Brownlee J. Antigen-antibody interaction[R]. Melbourne, Australia: Swinburne University of Technology, 2007.

[14] University of California, Irvine. The KDD cup 1999 data[EB/OL]. 1999-10-28. <http://kdd.ics.uci.edu/databases/kdd-cup99/kddcup99.html>.