文章编号:1671-4598(2016)07-0294-04 DOI:10.16526/j.cnki.11—4762/tp.2016.07.079 中图分类号:TP18 文献标识码:A

人工免疫危险理论中的平衡机制研究及应用

杨 超[1,2],张 龑[1,2],秦廷栋[1]
(1.湖北大学 计算机与信息工程学院,武汉 430062;2.湖北省教育信息化工程技术研究中心,武汉 430062)

摘要:危险理论作为人工免疫学的新兴研究方向,其主要思想是通过危险信号的发现和融合来检测异常,危险信号的自适应感知是人工免疫危险理论需要解决的首要问题;从生物免疫系统保障机体生理平衡这一机理出发,将免疫系统中的平衡思想引入危险理论中,通过寻找导致信息系统失衡的变化因素,来实现危险行为的自适应发现;从机体免疫平衡理论出发,借鉴数学中的微分方法对信息系统各种行为发生时资源的占用特征进行形式化描述;从信息系统资源指标占用特征入手,实现对信息系统中各种平衡的描述,通过对失衡状态的判定来进行危险的发现,并对其实现方法和步骤做出了解释;最后以僵尸程序(SpyBot)为实验对象验证了所提出的利用免疫平衡理论检测危险方法的有效性。

关键词:人工免疫系统;危险理论;平衡机制;数值微分

Research and Application of Immune Homeostasis Mechanism in Danger Theory

Yang Chao[1,2], Zhang Yan[1,2], Qin Tingdong[1]
(1. School of Computer Science and Information Engineering, Hubei University, Wuhan 430062, China;
2. Education Information Engineering Technology Research Center of Hubei Province, Wuhan 430065, China)

Abstract: Danger theory is a new research direction of artificial immune system. Its main idea is to detect anomalies by the discovery and fusion of danger signals. The adaptive perception of danger was the most important question need to be solved in Danger Theory. Based on the mechanism that the physiological balance was protected by biological immune system, the balance mechanism was introduced into Danger Theory in order to realize that the danger can be adaptive found through looking for changing factors which may lead to the imbalance of information system. This paper started from the immune homeostasis theory to formally describe the various characteristics of system resource indicators by using a differential calculus the balance in the information system was described in the feature of resource occupy. Besides, it is given the explanation of its meaning and implementation. Finally, use SpyBot as an example to test the effectiveness of the proposed method.

Keywords: artificial immune system; danger theory; homeostasis mechanism; differential calculus

0 引言

危险理论作为人工免疫学中一种新兴的理论方法,已经广泛应用于入侵检测[1-2]、机器学习[3]、数据挖掘[4]等各个研究领域,并取得了较好的研究成果。该理论针对传统免疫方法中SNS模式存在的self集合难以界定、self/nonself识别界限过于分明等固有缺陷所带来的伪肯定、伪否定率居高不下等问题[5],提出了利用危险信号代替“自我—非我”这种传统的定义模式来解释免疫学问题。

然而,危险理论自2002年引入计算机领域以来[6],其应用过程中也存在着危险来源和危险定义的不明确问题[7]。因此,在实际应用中,危险信号往往存在人工定义的痕迹,即根据已知经验将可能诱发危险的因素定义为导致危险发生的潜在危险信号[8-9]。

自适应性和多样性是免疫系统的基本特性[10]。危险理论目前这种依赖于人工经验的危险信号定义方法,削弱了其智能性,如何建立不依赖人工经验知识、自适应的感知危险和定义危险信号的方法是目前危险理论亟需解决的问题。生物免疫学中将免疫系统定义为:机体对外源物质的反应,其作用是识别和排除抗原性异物,以此来维持机体的稳定和生理平衡[11]。因此,免疫系统的本质特性应该是维护机体的生理平衡,阻止或消灭导致生物系统失衡的各种内外部变化因素。基于该思想,本文将免疫平衡机制引入到信息系统的危险感知中,分析了变化和平衡、平衡和危险之间存在的关系,同时以信息系统中资源指标的变化特征为例,通过对信息系统中平衡关系的刻画来判断各种“变化”是否对系统构成威胁,进而实现危险信号的自适应定义。

收稿日期:2016-04-10; **修回日期**:2016-05-05。
基金项目:湖北省教育厅中青年人才项目(Q2015001)。
作者简介:杨 超(1982-),男,湖北武汉人,博士,讲师,主要从事信息安全和人工免疫学方向的研究。

1 免疫平衡与免疫调节

机体免疫学中生理平衡(biological homeostasis)的概念是由Cannon首次提出的[12],他认为生理平衡就是机体在不断变化的内、外部环境中仍然保持稳定状态的一种能力。生物学中平衡的意义不是不变、固定,而是始终变化,但相对稳定的状态[13]。

Cohen的免疫模型认为:免疫系统的主要作用是修复并维持机体健康,为保证机体生理平衡,免疫系统必须根据机体状态不断调节免疫响应。该免疫响应不是简单对自我和非我的区分,而是根据变化对机体健康的影响来动态调节免疫响应[14]。

本节将对机体免疫学中平衡调节的核心思想及其具体实现机制进行介绍和分析,以此作为平衡理论在危险理论中应用的生物学基础。

免疫调节(Immunoregulation)是指机体识别和排除抗原性异物,维持自身生理动态平衡和相对稳定的机制。免疫调节机制不仅决定了免疫应答何时发生,也决定了免疫应答反应的强弱,是维持生理平衡的重要机制手段。

免疫调节通常是双向的,是指体内各种免疫细胞、免疫分子之间对免疫应答进行正、负两个方向的调节作用[15]。藉此来调节免疫应答的强度,以维持机体内部环境的相对稳定。这

种双向调节表现如下。

1）正向调节：在排除外来抗原异物时，刺激并加强免疫应答反应；

2）反向调节：清楚外来抗原物质后，及时减弱或终止免疫应答以尽量减少对自身组织的损伤。

T 细胞是免疫调节过程中的核心作用细胞，可分为杀伤 T 细胞（Killer T Cells，简称 Tk）和调节性 T 细胞两类。其中杀伤 T 细胞的主要功能是清除病毒、细菌和内部病变细胞等有害物质。

调节 T 细胞在免疫调节过程中起到至关重要的作用，调节 T 细胞通过分泌不同化学来促成上述的正负两个方向的调节作用。参与调节的 T 细胞可分为辅助性 T 细胞（helper T cells，简称 Th）和抑制性 T 细胞（suppressor T cells，简称 Ts）两类，其中辅助性 T 细胞与抗原结合刺激免疫应答，而抑制性 T 细胞则在免疫响应过程中，降低 T 细胞活性，反向抑制免疫应答。

从免疫调节机制可以看出，其正向和反向两种调节机制，构成了一个平衡控制系统（homeostatic control system）。该平衡控制系统的主要工作是：免疫系统受到有害物质入侵时，立即激活免疫应答以消灭有害物质，当这一过程完成后，立刻降低免疫应答的强度以免误伤正常细胞[16]。可以发现，免疫调节机制始终朝着免疫系统变化过程的相反方向进行作用，始终在延缓或者抑制免疫系统的变化，通过不断调节免疫应答的方向和强度来维持机体生理平衡，由此可以看出变化是导致免疫平衡被打破的关键因素。

2　变化与平衡的关系

软件是对客观世界中问题空间和解空间的具体描述，是对客观事物的一种反映，是知识的提炼和“固化”[17]。信息系统中各种功能的实现对应着系统资源的占用，不同的功能对系统资源的占用具有其各自特征，即各种软件操作行为和资源占用关系之间存在着一定的规律。这种规律保证了信息系统的正常运转，也表现为信息系统内、外部的一种平衡关系。保持这种平衡，系统各功能部件运转、调用正常，能够“齐心协力”完成特定的功能，反之，平衡的破坏会带来软件行为的异常。

变化是绝对的，不变是相对的。机体内部细胞的损伤、衰老、变异和死亡时刻发生，机体外部细菌、病毒时时企图入侵，直接威胁着机体健康。机体免疫系统依赖免疫防御、免疫自稳和免疫监视三大功能保证机体的正常运转[20]。这三大免疫功能高度和谐，共同抵御机体内部病变和外来抗原异物的侵害，保持自身免疫耐受以维持机体生理平衡。信息系统由于其固有的交互性，使得它与生命系统一样，时刻处于变化的过程中。对系统的任何操作都会带来各种性能指标的变化，有些变化来源于对系统的正常操作，而有些变化则预示着危险的来临。异常的变化，往往会带来系统调用、资源分配、时间占用等动态平衡的破坏。那些导致信息系统平衡被打破的变化因素，及其相互之间的关系是定义危险、分析危险的有效依据。

3　信息系统中的平衡描述

信息系统和生命系统一样是一个复杂的、交互式动态系统，信息系统正常运行时的操作对应着软、硬件系统资源的占用，这种资源占用关系为了支撑软件功能和操作行为，因而存在着一定的规律[17]，体现了信息系统的平衡。本文利用免疫系统的学习机制，通过对这种信息系统正常操作所表现出的资源占用特征的学习来建立信息系统平衡的描述模型，利用该模型能够实现信息系统平衡关系的刻画。通过对平衡关系的分析和失衡原因的捕获，来发现信息系统中的异常。

3.1　资源变化趋势的平衡

信息系统的平衡是一种动态的平衡，其中资源调用和软件行为的变化始终保持着特定的特征和规律。因此，对信息系统中资源占用的变化规律的描述，就是对信息系统平衡状态的刻画。

信息系统中，捕捉到的各种资源占用情况是以时间为单位的离散量，本文利用数值微分的方法来对这些离散的数据点进行分析和描述以刻画其变化趋势。数值微分的基本思想是，利用函数 $f(x)$ 在一系列离散点上的信息来近似构造一个简单函数 $g(x)$ 去逼近 $f(x)$，然后用 $g(x)$ 的微商去近似模拟 $f(x)$ 的微商，以此实现离散信息的连续描述。

其微商可用如下方法来表示[19]：

$$f'(x_i)_{right} \approx \frac{f(x_{i+1}) - f(x_i)}{h} \tag{1}$$

$$f'(x_i)_{left} \approx \frac{f(x_i) - f(x_{i-1})}{h} \tag{2}$$

公式（1）表示了一阶微商的向前差商近似，公式（2）表示了一阶微商的向后差商近似，其中 h 表示相邻离散信息点之间的距离，即 $x_{i+1} = x_i + h$，该距离可以表示为单位时间或者相邻事件。图 1 表示了 3 个离散数据点及其变化关系，利用数值微分的思想，可以将其以特征三元组 $\{f'(x_i)_{left}, f(x_i), f'(x_i)_{right}\}$ 的形式进行表现，该三元组中的 $f'(x_i)_{left}$ 和 $f'(x_i)_{right}$ 分别表示了特征信息点 x_i 左右两边曲线的变化趋势（即针对特征信息点的变化是上升、下降还是趋于平缓），类似于特征点与其前后样本信息点所组成的线段的斜率，其中 k_{i-1} 和 k_i 分别表示两个直线的斜率[20]。利用该特征三元组可以实现资源占用特征的描述，即实现了某一资源变化趋势的度量和平衡关系的刻画，如图 1。

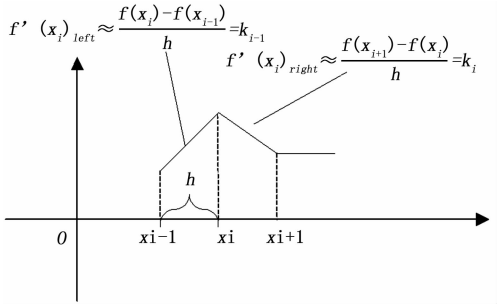

图 1　特征三元组中元素特征的图形化描述

3.2　状态失衡的判定

利用上节中的特征三元组描述法，可以实现对信息系统运行时资源占用变化特征的描述。由于信息系统中的资源占用均为离散的数据，因此可以利用曲线拟合函数来进行形式化描述，拟合函数的形式包括：多项式、幂指数等。

若系统状态发生变化，则这种资源占用指标的平衡关系会被打破，那么拟合函数的特征也会发生变化。数学中，常用导数来描述自变量和因变量在变化过程中的关系。因此，若指标间的平衡关系被打破，会表现在拟合函数导数的变化上，也就存在拟合函数导数的不一致情况，如公式（3）所示。

$$f'(x_t) \neq f'(x_0) \tag{3}$$

其中：$f(x_t)$ 表示时间状态 t 时刻，指标特征三元组所形成的拟合函数导数值，$f'(x_0)$ 表示作为比较样本的正常状态下指标特征三元组形成的拟合函数导数值。通过比较拟合函数导数值的变化，来判断状态是否发生变化，平衡是否打破。

4 实验

本实验的目的是在不依赖先验知识的情况下，以僵尸程序（SpyBot）为对象验证本文提出的利用免疫平衡理论检测危险方法的有效性。主要通过比较相同恶意软件和恶意行为在不同环境下对系统资源的占用是否存在相似的平衡特征来进行验证。

4.1 实验设计

本次实验采集的指标类型如表 1 所示，包括计算机的系统资源指标和网络资源指标两类。这两类指标作为僵尸程序分析的依据，不依赖于历史经验，根据两类指标的特征变化情况自适应的提取危险信号而忽略不产生突变的指标，因此并不需设置相应的权重值，见表 1。

表 1 采集指标列表

指标类型	指标名称	指标描述
系统级	PID	进程号
	P_Name	进程名
	P_Num	系统进程数量
	P_CPU	进程 CPU 占用率
	P_Mem	进程内存占用率
网络级	TCP_Packets	每秒内发送/接收到的 TCP 包数量
	UDP_Packets	每秒内发送/接收到的 UDP 包数量
	ARP_Packets	每秒内发送/接收到的 ARP 包数量
	ICMP_Packets	每秒内发送/接收到的 ICMP 包数量
	IRC_Packets	每秒内发送/接收到的 IRC 包数量

实验将对僵尸程序在进行恶意行为操作时的资源占用情况进行记录，以此作为后续分析的依据，其步骤可总结如下：

1）潜伏阶段：在主机中植入僵尸程序，但此时僵尸处于休眠阶段，不进行任何恶意操作；

2）唤醒阶段：攻击者向僵尸主机发送命令以唤醒僵尸主机；

3）键盘侦听：攻击者命令僵尸程序监听用户击键函数令，并远程将键盘输入信息传递给攻击者；

4）系统进程扫描：僵尸程序扫描主机系统当前正在运行的进程，并将结果传递给攻击者；

5）切断进程行为：攻击者命令僵尸程序终止主机上正在运行的程序；

6）停止恶意行为，退出僵尸程序。

4.2 实验分析

本次试验中，在两台不同的机器上部署了僵尸程序，以僵尸程序处在潜伏阶段 IRC 包的变化情况为例，比较僵尸程序在两个机器上表现出的特征是否相同或相似。

图 2 展示了在不同的主机 A 和 B 上运行僵尸程序时，IRC 数据包的占用情况。其中主要采集了执行 4.1 节中所介绍的实验流程中的第 2～5 步，共 4 个操作步骤，3 种恶意行为的 IRC 数据包。从图上可以看出，两个主机上运行僵尸程序时，IRC 数据包的占用情况不同，但整体趋势和特征大体相同，如图 2。

以僵尸处在未激活的潜伏状态下时，IRC 数据包占用情况为例，利用前面所介绍的特征三元组方法来描述其运行特征，对数据进行拟合得到如图 3。

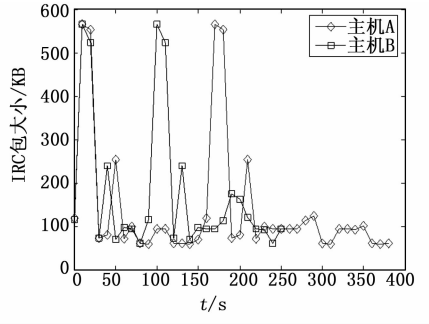

图 2 僵尸程序运行时 IRC 数据包占用情况

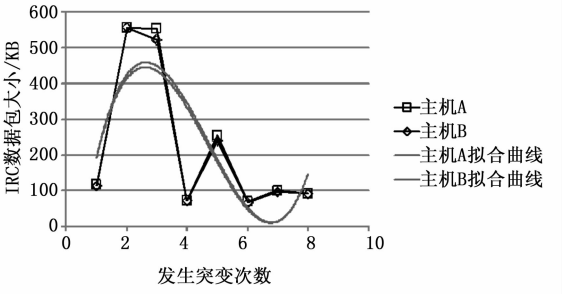

图 3 僵尸程序潜伏阶段不同主机的 IRC 占用特征

在该图中，仅关注 IRC 数据包发生突变时的状态，而忽略其中一般性的变化，可以发现在相同恶意行为发生时，两台主机上 IRC 数据包的占用特征基本相同，利用三次方多项式进行拟合后得到的拟合函数分别为：

$$y = 12.492x^3 - 176.77x^2 + 672.26x - 313.86 \quad (5)$$

$$y = 12.182x^3 - 171.73x^2 + 649.57x - 296.43 \quad (6)$$

通过分析可以发现，不同主机上僵尸程序对资源占用情况所描述出的拟合函数特征相似，对拟合函数求导后特征基本相同。即在相同恶意行为发生时，恶意行为所需要调用的系统资源满足一定规律，构成了一个平衡关系。当不同恶意行为发生时，其恶意特征所构成的平衡关系是不同的。

根据该实验结果可以推知，若在免疫系统的学习阶段建立正常行为的平衡关系模型，就能够在不依赖先验知识的情况下，通过捕捉平衡是否被打破来判断是否有危险产生。

5 结论

本文从生物免疫系统保障机体生理平衡这一机理出发，将免疫系统中的平衡思想引入危险理论中，通过寻找导致信息系统失衡的变化因素，来实现危险的自适应发现。通过对软件正常运行过程中，对各种资源指标的占用情况及其之间关系的描述和刻画来描述信息系统的平衡状态，通过捕捉导致系统失衡的因素来实现危险的自适应感知。借鉴数学中微分的思想，构造出系统资源及其相互关系的形式化描述方法，以实现系统运行状态的表达。希望以此为基础，建立基于资源关系特征的变化比较方法来发现软件的异常，为危险理论中危险信号的自适应定义提供一条新的思路。

本文对上述方法的可行性进行了一些理论上的研究和初步的实验验证，下一步将更进一步增加实验用例，对该方法的适用范围和执行效率进行更深入的研究。

参考文献：

[1] Vella M, Roper M, Terzis S. Danger theory and intrusion detection: possibilities and limitations of the analogy [C]. Proceedings

of the 9th International Conference on Artificial Immune Systems. Springer，2010：276－289.
[2] Greensmith J，Aickelin U. Dendritic cells for SYN scan detection [A]. Proceedings of the 9th Annual Conference on Genetic and Evolutionary Computation [C]. New York：ACM，2007：49－56.
[3] Zhu Y，Tan Y. A danger theory inspired learning model and its application to spam detection [J]. Advances in Swarm Intelligence Lecture Notes in Computer Science，2011，6728：382－389.
[4] Secker A，Freitasa A，Timmis J. A danger theory inspired approach to web mining [A]. Proceedings of 2th International Conference on Artificial Immune Systems [C]. Heidelberg：Springer，2003：156－167.
[5] Kim J，Bentley P，Aickelin U，et al. Immune system approaches to intrusion detection－a review [J]. Natural Computing，2007，6 (4)：413－466.
[6] Aickelin U，Cayzer S. The danger theory and its application to artificial immune systems [A]. Proceedings of the 1st International Conference on Artificial Immune Systems [C]. Heidelberg：Springer，2002：141－148.
[7] Aickelin，Bentley P，Cayzer S，et al. Danger theory：the link between AIS and IDS [A]. Proceedings of the 2nd International Conference on Artificial Immune Systems [C]. Heidelberg：Springer，2003：147－155.
[8] Al－Hammad Y，Aickelin U，Greensmith J. DCA for bot detection [C]. Proceedings of IEEE Congress on Evolutionary Computation. Washington DC：IEEE Computer Society，2008：1807－1816.
[9] Greensmith J，Aickelin U，Tedesco G. Information fusion for anomaly detection with the dendritic cell algorithm [J]. Information Fusion，2010，11 (1)：21－34.
[10] 莫宏伟，左兴权. 人工免疫系统 [M]. 北京：科学出版社，2009.
[11] 陈慰峰. 医学免疫学 [M]. 北京：人民卫生出版社，2000.
[12] Cannon W B. The wisdom of the body [M]. New York：Norton，1932.
[13] Owens N，Timmes J，Greensmith J，et al. On immune inspired homeostasis for electronic systems [C]. Proceedings of 6th International Conference on Artificial Immune Systems. Heidelberg：Springer，2007：216－227.
[14] Cohen I R. Tending Adams garden：evolving the cognitive immune self [M]. Amsterdam：Elsevier Academic Press，2000.
[15] Tew J，Phipps P，Mandel T. The maintenance and regulation of the humoral immune response：persisting antigen and the role of follicular antigen－binding dendritic cells [J]. Immunological Review，1980，53：175－211.
[16] Delves P，Martin S，Burton D，et al. Roitt’s essential immunology [M]. 12nd ed. USA：Wiley－Blackwell，2011：15－25.
[17] 杨芙清. 软件工程技术发展思索 [J]. 软件学报，2005，16 (1)：1－7.
[18] Widmaier E P，Raff H，Strang K T. Vander’s human physiology：The mechanisms of body function [M]. 10th ed. USA：Mc－Graw Hill，2006：100－125.
[19] 周　铁. 计算方法 [M]. 北京：清华大学出版社，2006.
[20] Yang C，Liang Y W，Liu A. The danger sensed method by feature changes [J]. Energy Procedia，2011 (13)：4429－443.

(上接第 293 页)

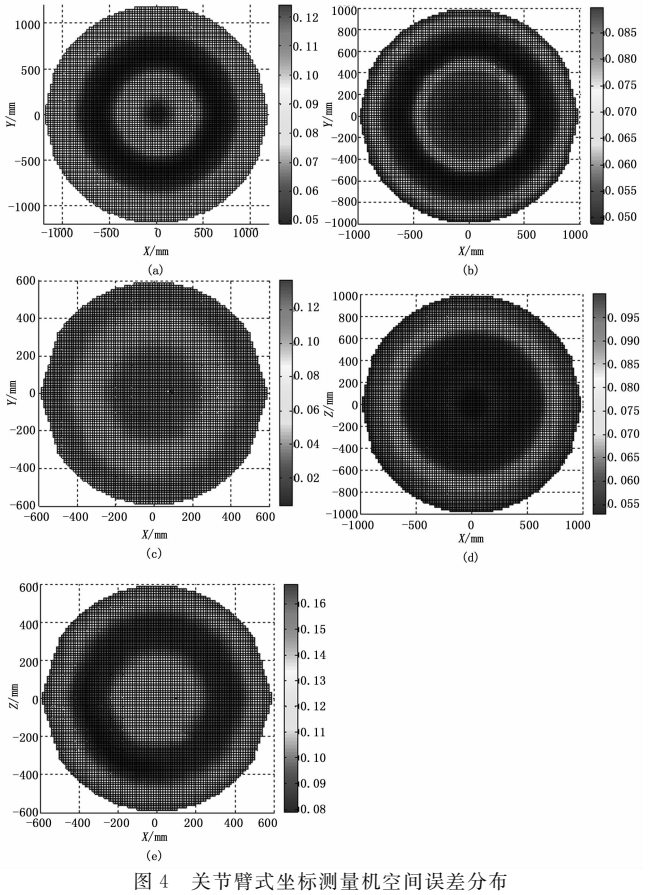

图 4　关节臂式坐标测量机空间误差分布

阈值，提高其收敛速度和运算速度，实验证明：BP 神经网络和 PSO－BP 神经网络都可以对关节臂式坐标测量机的空间误差进行预测，PSO－BP 神经网络模型预测精度更高，具有理想的可靠性，并利用 PSO－BP 神经网络对对关节臂式坐标测量机的空间误差进行预测，用 MATLAB 绘制出其空间误差分布，在其测量空间范围内得出其误差分布的规律，在实际的测量应用中，可以避开其测量精度较小，误差较大的区域，具有现实指导作用。

参考文献：

[1] 裘祖荣，孙增玉，张国雄. 关节臂式坐标测量机标定系统的设计 [J]. 计算机测量与控制，2009，17 (1)：88－90.
[2] Santolaria J，Yagüe J A，Jiménez R，et al. Calibration－based thermal error model for articulated arm coordinate measuring machines [J]. Precision Engineering，2009，33 (4)：476－485.
[3] 汪平平，费业泰，尚　平，等. 柔性坐标测量机参数辨识方法 [J]. 农业机械学报，2007，38 (7) 129－132.
[4] 郑大腾. 柔性坐标测量机空间误差模型及最佳测量区研究 [D]. 合肥：合肥工业大学，2010.
[5] 高贯斌，王　文，林　锲，等. 关节臂式坐标测量机误差仿真系统建模与分析 [J]. 计算机集成制造系统，2009，15 (8)：1534－1540.
[6] 何晓凤. 基于 PSO—BP 神经网络的混凝土抗压强度预测 [J]. 微型机与应用，2011，30 (20)：87－90.
[7] 李　敏. 基于粒子群优化神经网络的刀具磨损状态监测技术研究 [D]. 成都：西南交通大学，2012.
[8] 王　亮，张宏伟，岳　琳，等. PSO－BP 模型在城市用水量短期预测中的应用 [J]. 系统工程理论与实践，2007，27 (9)：165－170.