模块化免疫神经网络的模型研究

侯家利[1,2],朱梅阶[2],彭 宏[2]
(1. 东莞理工学院软件学院,广东东莞 523106;2. 华南理工大学计算机学院,广东广州 510641)

摘 要: 本文讨论了免疫网络 *I* 和神经网络 *N* 的相互作用,利用神经网络的聚类特性,提出了一种新的安全模型——模块化免疫神经网络模型,并对其中的信号进行了有效的分类和相应的处理,同时根据模型中两大网络的作用机理,给出了它们之间的作用算法,最终形成了一个动态平衡的、自适应的、分布式的网络模型.

关键词: 拓扑结构; 信号分类; 相互作用; 特征分析
中图分类号: TP183 **文献标识码**: A **文章编号**: 0372-2112 (2005) 08-1502-04

Research on Modular-Based Immune Neural Network Model

HOU Jia-li[1,2], ZHU Mei-jie[2], PENG Hong[2]
(1. *Software College, Dongguan University of Technology, Dongguan, Guangdong* 523106, *China*;
2. *Computer Engineering & Science Dept, South China University of Tech, Guangzhou, Guangdong* 510641, *China*)

Abstract: The authors discussed the mutual mechanism between immune and neural networks. In terms of the cluster particularity of neural network, they built up a new security model —modular immune neural network, then classified and handled its original and input data with it, and constructed three algorithms from their mutual mechanisms, which forms a homeostic, auto-adaptable and distributed model.

Key words: topology structure; data classification; mutual mechanisms; character analysis

1 引言

随着信息技术的发展和互联网应用的不断普及,网络安全正受到日益严重的威胁.传统的安全措施已不能保证网络系统的安全,迫切需要用新的技术解决网络安全问题.为此许多学者进行了一些探讨,91 年 H H Yan 在文献 1 中利用电压差的方法设计了一个二层的神经网络,它能将系统中处理的信号分成三类:常态、警惕态和危险态;96 年 Mahmoud 在文献[2]中利用特征空间中的模式训练一个分类器,分类器可将系统中处理信号分成两类:安全类和不安全类.虽然后来这方面的研究很不够,但是,在某些应用领域,利用神经网络对一些具体问题的安全进行许多有益的研究,取得丰硕的成果,特别是人工免疫系统成为研究热点以来,不少学者利用免疫学理论对安全问题也进行了一些研究和讨论,提出了多种人工免疫模型的算法,Tarakanov[3]基于免疫系统中抗体和抗原的相互作用原理建立了免疫系统的数学模型,Zak[4]模拟免疫系统功能提出了免疫系统的随机模型,这种模型具有自己非己识别、自修复等功能,Forrest[5]基于反相选择原理提出了反相选择算法,用于异常检测,然而,安全问题的研究还很不够,还存在着诸多的问题:(1)综合利用神经网络和免疫网络还未正式给出过解决计算机安全的模型;(2)即使在文[1]、文[2]中给出了利用神经网络对系统处理的信号进行分类的方法,但对分类的信号如何处理并未解决,而且分类方法还不具有一般性;(3)神经网络和免疫网络对安全的研究彼此是独立的、脱节的、分散的,相互之间的作用关系没有进行过任何的讨论,更谈不上形成一个完备解决安全的方案.

针对以上问题,结合神经网络优化、聚类的特点、免疫网络识别自己、非己和抗体处理抗原的机理以及遗传算法中适者生存和优胜劣汰的原理,提出了一种新的计算机系统安全模型,该模型能动态实现系统处理信号的分类,而且对每类信号也给出了综合有效的处理方法,同时也指出并利用了神经网络和免疫网络相互作用的规律,最终形成了一个动态的、自适应的、分布式的安全模型.分析表明该模型能有效地解决网络安全问题,特别在实时系统中解决计算机安全有很大潜力和发展空间.

2 模块化免疫神经网络的模型概述

2.1 模块化神经网络

模块化神经网络是包括了多个子模块的神经网络,每个子模块完成神经网络全局任务中的一个子任务或一部分,所有子模块的输出经过任务合成后得到系统最后的输出.

层次模块化神经网络[6](HMNN)由任务分解单元 TDU

收稿日期:2004-07-12;修回日期:2005-04-27
基金项目:国家自然科学基金重点项目(No. 30230350);广州市科技攻关项目(No. 2004Z2 - D0091);广东省科技攻关项目(No. 2004A10202001)

(tast decomposition unit)、子任务处理单元 STUP(sub-task processing unit)和结论合成单元 CSU(conclusion synthesis unit)组成.其中子任务处理单元是由多个神经网络并行组成的一个小的神经网络系统.

其基本思想是,在学习阶段,TDU 将学习样本空间分解成若干样本子空间,针对每个子空间构造一个 STUP 并进行学习.在工作阶段,TDU 用来判定数据对于各子空间的隶属度,由 CSU 根据隶属度动态选取部分或全部 STUP 进行工作,并将选用的 STPU 的处理结果以加权和的方式集成.

2.2　生物免疫系统的信息处理机理

生物免疫系统由免疫器官、免疫组织以及多种淋巴细胞组成,淋巴细胞主要包括 T 细胞和 B 细胞两种,它们分布于整个身体,在免疫中起主要作用,B 细胞可以分泌抗体,辅助 T 细胞刺激或抑制 B 细胞抗体的分泌.当病原体侵入机体后,被一些 B 细胞识别,这些 B 细胞在 T 细胞的作用下分裂,进而变成浆细胞,分泌抗体来消灭抗原,发生免疫应答.免疫系统中的信息处理机理包括以下几方面:

(1)识别自己与非己:免疫系统的反向原理[6]表明,免疫系统能够识别体内分子与外来分子.

(2)学习与优化:免疫网络和克隆选择理论揭示了免疫应答过程的机理,表明抗体的产生是免疫系统的学习过程[7],也是一个优化过程.

(3)联想与记忆:免疫系统消灭抗原后,产生记忆细胞,当与该抗原相似的抗原再次入侵机体时,免疫系统能产生最快速、更强烈的二次应答,免疫记忆是一种联想记忆[7].

(4)自适应网络:免疫网络学说[8]表明,免疫系统中的 B 细胞通过识别与被识别组成一个网络,对抗原的识别是网络中的 B 细胞相互作用的结果,免疫网络与神经网络一样,是一个能够学习的和记忆的自适应网络.

(5)并行的分布系统:免疫系统中的淋巴细胞分布于全身,根椐周围的环境自适应地确定自身的行为,整个免疫系统是一个没有控制中心的并行的分布自治系统.

(6)复杂系统:免疫系统本身是一个具有"突现智能"的复杂系统.

2.3　处理单元的拓扑结构与信号处理机理

处理单元(如图 1 所示)由两个网络构成,一个是免疫网络,另一个是多层神经网络.免疫网络分局域免疫网络(如图 1 所示)和全局免疫网络,同样多层神经网络也有全局和局域之分;其中全局免疫网络由所有局域免疫网络组成,全局多层神经网络由所有局域多层神经网络组成.免疫网络随多层神经网络的作用决定是否有应答,应答的免疫网络则根据唤醒的免疫系统中记忆细胞的不同种类,而产生不同的决定因子(细胞因子或抗体)并作用于神经网络,而多层神经网络,它的输入信号与局域免疫网络抗体基因(决定因子)进行匹配,若匹配度低于整个阈值时,则多层神经网络中抗原(源信号)被淘汰,若高于整个阈值时,则抗原(源信号)激活各神经元,使之处于兴奋状态,输出信号.模型中的整个过程不断循环,形成一个螺旋链式结构.每一个过程都有反馈,经过不断反馈,调整以达到最理想的状态.图中字符 I, N 分别表示免疫网络和多层神经网络,$\zeta\lambda\cdots\mu$ 是神经网络产生的作用因子(不同的抗原产生不同的因子,不同的因子对 I 产生的作用不同),$\alpha\beta\cdots\gamma$ 是免疫网络系统产生的细胞因子(或抗体),它们对 N 进行调节和控制.

2.4　模块化免疫神经网络原理

处理单元(如图 1 所示)由局域神经网络 N 和局域免疫网络 I 所组成,模块化免疫神经网络由许多处理单元构成(如图 2 所示).局域网络的工作原理描述如下:当处理单元中的神经网络 N 各输入与其权值的积和 $\sum w\cdot X(t)$ 超过兴奋阈值 θ_2 时,神经元直接进入兴奋状态,并输出电脉冲,此时输入信号可接收(被记忆或已有记忆).当处理单元中多层神经网络 N 的输入与其权值的积和 $\sum w\cdot X(t)$ 低于抑制阈值 θ_1 时,神经元处理于抑制状态,此时输入信号被拒绝接收,即不可记忆.

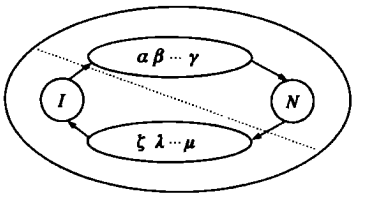

图 1　处理单元的构成示意图

当处理单元中神经网络 N 的输入与其权值的积和 $\sum w\cdot X(t)$ 位于区间 $[\theta_1,\theta_2]$ 时,神经元处于可疑态,此时处理单元中多层神经网络 N 便产生作用因子 $\xi\lambda\cdots\mu$ 对局域免疫网络进行作用(激活局域免疫网络系统 I),致使 I 产生抗体 $\alpha\beta\cdots\gamma$,如果抗体基因与抗原(源信号)基因匹配度高的,则产生细胞因子刺激神经元,使神经元兴奋,从而间接的达到是否好象是抗原使神经元兴奋,这样源信号便可被接收;如抗体基因与抗原(源信号)基因匹配度低,则产生细胞因子刺激神经元,使神经元抑制,从而间接的达到是否好象是抗原使神经元抑制,这样抗原(源信号)便可丢掉.上述是处理单元中局域神经网络 N 和处理单元中的局域免疫网络 I 相互作用的原理,对于全局网络(图 2 所示),其原理是一致的,在此就不赘述.

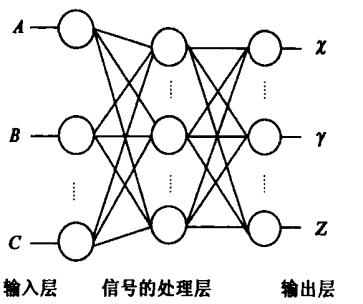

图 2　模块化免疫神经网络的模型

2.5　模块化免疫神经网络的模型

模块化免疫神经网络的模型(如图 2 所示)由三层组成,第一层为输入层,由接收输入信号的许多处理单元(即多层神经网络)构成;第二层为信号的处理层,根据输入信号决定处理单元是否处于激活、抑制或非常态以及各状态下信号是如何处理的;第三层为输出层,它根据第二层的结果决定处理单元的输出类型.

2.5.1　处理单元基元(神经元)激活、抑制机理　假设一处理单元中有 K 个神经元 $\lambda=\{A_1,A_2,\cdots,A_K\}$,其信号输入为:$X=\{X_1,X_2,\cdots,X_K\}$,设某神经元 A_j 具有输入,各输入信号的强度分别为:$X_j=\{x_{i1},x_{i2},\cdots,x_{iN}\}$,这个处理单元的输出是 Y_i,则处理单元中神经元的工作原理可由式(1)所示的离散时

间差分方程描述:

$$Yi(t+\Delta t) = \mathrm{Esgn}[\sum w \cdot X(t) - \theta] \quad (1)$$

式中 $t = 0, 1, 2, \cdots$; Δt 是输入、处理的持续时间; $w = [w_1, w_2, \cdots\cdots w_N]^{\mathrm{T}}$, $\theta = [\theta_1, \theta_2, \cdots\cdots, \theta_k]^{\mathrm{T}}$ 为神经元阈值向量, $\theta_i \subseteq [\theta_1, \theta_2]$.

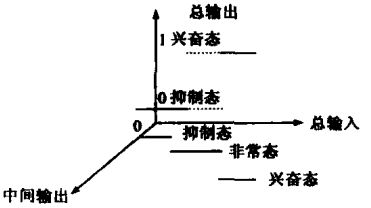

图 3 神经元的输出函数

函数 Esgn 为扩展的阶跃函数(如图 3 所示),由下式表示:

$$Esgn[u] = \begin{cases} 0, & u < \theta_1 \\ q, & \theta_1 \le u \le \theta_2 \\ 1, & u > \theta_2 \end{cases} \quad (2)$$

$$Sgn[q] = \begin{cases} 0, & q < \theta_1 \\ 1, & q > \theta_2 \end{cases} \quad (3)$$

其中: $q \in (0, 1)$

即神经元最终的输入、输出取值为 0, 1. 1 代表神经元的兴奋状态, 0 代表神经元的抑制状态. 输出 q 值是一种中间的过渡态,经过免疫系统作用后,要么部分转换成兴奋态,要么部分转换成抑制态.

区间: $[\theta_1, \theta_2]$ 为神经元的阈值区间. 当各输入与其权值积和 $\sum w \cdot X(t)$ 超过 θ_2 时,神经元进入兴奋态,输出电脉冲.

2.5.2 输出信号的安全分类

我们令变量 $u = \frac{1}{1+d}$, 输出的信号可按下列函数值分类:

若函数值位于区间 $(\theta_2, 1]$, 则输出的信号 $Esgn(u)$ 处于安全态;

若函数值位于区间 $(0, \theta_1]$, 则输出的信号 $Esgn(u)$ 处于不安全态;

若函数值位于区间 $(\theta_1, \theta_2]$, 则输出的信号 $Esgn(u)$ 处于可疑态;

其中 d 表示模型中神经网络输出信号和期望输出信号的海明距离,安全态、不安全态、可疑态分别是神经元处于各状态时信号的输出分类.

3 免疫网络 I 和神经网络 N 的作用规则

3.1 免疫网络 I 对神经网络 N 的调控

(1) 免疫网络 I 优化神经网络 N 权值对其实施调控

I 网络产生的抗体或激活 I 中记忆细胞所获取的抗体,根据抗体类型(或模糊距离为 d) 构造适应度函数和目标函数,通过对 N 网络连接权值 $w_{ji}, \cdots\cdots, w_{ml}$ 调整,使 N 网络达到要求. 具体算法如下:

(a) 构造适应度函数: $u = \frac{1}{1+d}$ (4)

目标函数由式(1)给出.

(b) 产生染色体基因码集. 例如:当前的神经网络权值为 w_{ji}, w_{sr} $\cdots\cdots$, w_{ml} 分别由二进制串 011011110101000, 111001011111100, ……,100101110101100 组成种群.

(c) 对种群中的每一个体利用式(4)进行评估.

(d) 根据评估结果(是否满足终止条件,满足终止条件优化结束,否则转到第(g)步,直到满足终止条件为止) 决定是否到第(g)步.

(e) 利用选择操作产生新的种群. 根据个体适应度按概率比例从当前种群中选取个体.

(f) 通过遗传变异产生新的个体,在种群中用后代代替父代.

(g) 用突变概率随机选择个体,然后返回到第(c)步.

(2) I 网络产生的抗体对 N 网络的输入信号进行的处理

N 网络中的可疑信号或不安全信号作为抗原出现在 I 网络中,免疫网络响应,免疫网络对抗原进行识别,并用产生的免疫效应因子与抗原作用,将其破坏、清除等. 具体算法描述如下:

(a) 免疫网络 I 识别入侵的抗原,包括抗原的类型(输入信号的种类).

(b) 从记忆细胞中获取抗体.

(c) 计算抗体之间的亲合度,亲合度 η_k 由等式(5)给出:

$$\eta_k = m_{\phi k} / \sigma_k \quad (5)$$

$m_{\phi k}$ 表示抗体 ϕ 和抗体 k 之间的亲合力,亲合力 σ_k 利用式(6)寻求最优解:

σ_k = 与 $m_{\phi k}$ 一样具有相同亲合力的抗体总和/抗体总和 (6)

我们可用相同的方法计算出抗体与抗体之间的亲合度 η_k. 同时与抗原匹配度高的抗体将被分散到记忆细胞中,以便对下次入侵抗原迅速地免疫应答.

(d) 抗体的激活和抑制

利用式(5)免疫网络 I 能控制记忆细胞中抗体浓度为 η_k 的种种抗体. 假若某类抗体获得较高的亲合力,则该类抗体被激话,激活的抗体将有效处理抗原,将其破坏,清除. 然而过高浓度 η_k(即不明抗原或亲合力差的抗原) 的情况,则转到第(e)步. 过低浓度 η_k,则抗体自行死亡,不再对抗原起作用.

(e) 新抗体的产生

对不明抗原,免疫网络 I 将产生新的抗体. 抗体可通过遗传操作(突变或交叉或选择) 产生. 这些操作过程可以产生较为理想的抗体. 然后转到第(d)步.

3.2 N 网络对 I 网络的作用

抗原一出现免疫网络便应答,抗原对 B 细胞的激活级不仅依赖于与抗原的匹配度,而且还依赖于与免疫网络中其他 B 细胞的匹配度. 假若浓度 η_k 过低,那么 B 细胞死亡;假若浓度 η_k 较高,则该类抗体被激话,激活的抗体将有效处理抗原,将其破坏,清除;假若浓度 η_k 过高,此时抗体处于抑制状态,需要产生新的抗体对抗原作用. 具体算法描述如下:

(1) N 网络的输入信号 x_i 和输入层与信号的处理层处理单元的连接权值 w_{ji} 在目标函数的作用下,输出信号 Y_i,即:

$$Yi(t+\Delta t) = Esgn[\sum w \cdot X(t) - \theta] \quad (7)$$

(2) 将输出信号 Y_i 作为抗原作用 I 网络.

(3) 根据式(5)计算抗原 Y_i 和 I 网络抗体的浓度 η_k.

(4) 假若浓度 η_k 过低,那么 B 细胞死亡;假若浓度 η_k 较高,则该类抗体被激活,激活的抗体将有效处理抗原,将其破

坏,清除;假若浓度 η_k 过高,则转到第(e)步.

(5)新抗体的产生　对于不明抗原,免疫网络 I 将产生新的抗体,经过优化后,有效的抗体将分散到记忆细胞中.

4　模型的特征分析

与传统网络相比较,该模型有如下优点:

(1)健壮性　免疫功能通过免疫网络来实现,没有控制中心或协同中心,信息的处理依靠大量神经元或抗体同时协同作用来完成.即使某一个体可能是随机的,不可靠的,但局部免疫功能失常不会导致整个网络的免疫崩溃.因此,模型整体上是健壮的分布式安全处理模型;

(2)多层次性与多样性　模型具有多个防御层次.抗原的种类繁多,千差万别,免疫网络的识别多样性,可以让少量的抗体经过变异去匹配数量比它多得多的抗原.所以网络模型具有多层次的多样性的防护措施.

(3)自适应性和记忆性　该网络模型具有很强的自适应能力,能准确识别并消灭抗原性异物,保护自身,也就是说网络模型根据环境的变化自动调节权值,使网络的行为适应规定的任务,而且模型中的免疫网络能利用记忆细胞获取抗体,抗体迅速增殖后杀死抗原.

(4)动态平衡性　免疫网络中各种抗原与抗体,抗体与抗体之间相互促进或抑制,自我调节,组成一个动态的神经免疫网络.

5　结束语

本文借助神经网络、免疫学和遗传算法理论给出了一种新型的网络安全模型,与传统网络相比较,显现出诸多的优越性,具有良好的发展前景和强大的生命力.下一步我们准备在安全信号分类,免疫学习算法,神经网络 N 和免疫网络 I 相互作用规则以及抗体激活阈值的确定等方面进行研究,以形成一个完备的免疫神经网络模型.

参考文献:

[1] Yan, H H, Chow, J C, Kam M, Sepich C R, Fischl r. Design of a binary neural network for security classification in power system operation [A]. Proceedings-IEEE International Symposium on Circuits and Systems[C]. Singapore, 1991, Singapore, 1991. 1121 - 1124.

[2] Zayan, Mahmoud B, El-Sharkawi, Mohamed A, Prasad, Nadipuram R. Comparative study of feature extraction techniques for neutral network classifier[A]. Proceedings of the International Conference on Intelligent Systems Applications to Power Systems[C]. Orlando, FL, USA, ISAP, 1996. 400 - 404.

[3] Tarakanov A, Dasgupta D. A formal model of an artificial immune system[J]. Biosystem, 2000, 55(1 - 3): 151 - 158.

[4] Zak M. Physical model of immune inspired computing[J]. Information Sciences, 2000, 129(1 - 4): 61 - 79.

[5] Forrest S, Pereison A S, Alien I, Cherukurj R Self-nonself discrimination in a Computer[A]. In Priceedings of IEEE Symposium on Research in Security and Privacy[C]. Oakland, 1994. 202 - 212.

[6] 魏崴,王攀,等.层次化神经网络新方法研究[J].武汉理工大学学报,2003,25(6):23 - 26.
Wei Wei, Wang pan. A novel algorithm for hierachical modular neural network[J]. J Journal of Wuhan University of Technology, 2003, 25(6): 23 - 26. (Chinese Source)

[7] Kim, Dong, Hwa, Lee, Kyu. Young Neural networks control by immune network algorithm based auto-weight function tuning[A]. 2002 International Joint Conference on Neural Networks (IJCNN '02), Proceedings of the International Joint Conference on Neural Networks[C]. Honolulu, HI Sponsor: IEEE, NNS, INNS, 2002. 1469 - 1474.

[8] De Castro I N, Von Zuben F J. The clinal selection algorithm with engineering applications[A]. Genetic and evolutionary computation conference[C]. Las Vegas, USA, 2000. 36 - 37.

作者简介:

侯家利　男,副教授,硕士,主要研究方向为模块化神经网络、计算机安全. E-mail: houjl@dgut.edu.cn.

彭　宏　男,教授,博士生导师,主要研究方向为模块化神经网络.

朱梅阶　男,1999 年浙江大学理学院毕业,获硕士学位,现工作于华南农业大学信息学院,主要研究兴趣在人工智能、数据挖掘等方面,近几年发表文章 5 篇,其中 EI 收录 2 篇.